



Email Security

версия 5.30

Руководство по внедрению

© Positive Technologies, 2026.

Настоящий документ является собственностью Positive Technologies и защищен законодательством Российской Федерации и международными соглашениями об авторских правах и интеллектуальной собственности.

Копирование документа либо его фрагментов в любой форме, распространение, в том числе в переводе, а также их передача третьим лицам возможны только с письменного разрешения Positive Technologies.

Документ может быть изменен без предварительного уведомления.

Товарные знаки, использованные в тексте, приведены исключительно в информационных целях, исключительные права на них принадлежат соответствующим правообладателям.

Дата редакции документа: 06.02.2026

Содержание

1.	Об этом документе.....	5
1.1.	Условные обозначения.....	5
1.2.	Другие источники информации о PT Email Security.....	6
2.	О PT Email Security.....	7
3.	Выбор конфигурации PT Email Security.....	9
4.	Выбор лицензии PT Email Security.....	12
5.	Требования к узлам PT Email Security.....	13
5.1.	Аппаратные требования.....	13
5.2.	Программные требования.....	17
5.2.1.	Требования к настройке BIOS и UEFI.....	18
5.2.2.	Требования к разметке жесткого диска.....	19
5.2.3.	Требования к ОС для развертывания с помощью установщика.....	22
5.2.4.	Особенности развертывания в виртуальной среде.....	23
5.3.	Требования к сетевой инфраструктуре.....	24
6.	Установка локального сервера обновлений.....	34
6.1.	Аппаратные и программные требования.....	36
6.2.	Установка локального сервера обновлений.....	37
6.3.	Настройка локального сервера обновлений.....	39
6.4.	Активация лицензии.....	45
6.5.	Перенос обновлений в изолированный сегмент сети.....	45
6.6.	Выбор локального сервера в качестве источника обновлений.....	47
7.	Развертывание PT Email Security с помощью установщика.....	50
7.1.	Подготовка к развертыванию.....	51
7.1.1.	Проверка доступа к серверам обслуживания.....	51
7.1.2.	Распаковка архива с установщиком.....	51
7.1.3.	Настройка подключения менеджера обновлений ОС к прокси-серверу.....	52
7.2.	Базовая конфигурация.....	52
7.2.1.	Установка гипервизора Xen на основной узел.....	53
7.2.2.	Установка компонентов PT Email Security на основной узел.....	54
7.3.	Высоконагруженная конфигурация.....	55
7.3.1.	Установка компонентов PT Email Security на основной узел.....	55
7.3.2.	Установка гипервизора Xen на дополнительный узел.....	56
7.3.3.	Установка компонентов PT Email Security на дополнительный узел.....	57
7.4.	Отказоустойчивый кластер для высоконагруженной конфигурации.....	59
7.4.1.	Установка службы Keeralived на основной или резервный узел.....	59
7.4.2.	Установка компонентов PT Email Security на основной узел.....	60
7.4.3.	Установка компонентов PT Email Security на резервный узел.....	61
7.4.4.	Установка гипервизора Xen на дополнительный узел.....	62
7.4.5.	Установка компонентов PT Email Security на дополнительный узел.....	63
7.5.	Дополнительные действия при развертывании.....	64
8.	Первоначальная настройка PT Email Security.....	68
8.1.	Настройка доменного имени PT Email Security.....	68
8.2.	Добавление адресов для доступа к веб-интерфейсу PT Email Security.....	69

8.3.	Настройка подключения к прокси-серверу	69
8.4.	Настройка подключения к прокси-серверу с SSL-инспекцией	71
8.5.	Активация и замена лицензии PT Email Security	72
8.6.	Подключение внешнего PT MC.....	73
8.7.	Установка доверенного SSL-сертификата	74
8.8.	Отключение передачи информации о работе PT Email Security.....	75
9.	Изменение конфигурации PT Email Security	76
9.1.	Исключение дополнительного узла из конфигурации PT Email Security.....	76
9.2.	Удаление с узла гипервизора Xen	77
9.3.	Удаление с узла компонентов PT Email Security	77
10.	О технической поддержке	78

1. Об этом документе

Руководство по внедрению содержит информацию для планирования и выполнения развертывания Positive Technologies Email Security (далее также — PT Email Security) в инфраструктуре организации. В руководстве вы найдете описание типовых конфигураций PT Email Security, а также инструкции по установке и первоначальной настройке продукта.

Руководство адресовано руководителям и специалистам IT-подразделения организации, которые планируют и выполняют развертывание PT Email Security.

Комплект документации PT Email Security включает в себя следующие документы:

- Этот документ.
- Руководство администратора — содержит справочную информацию и инструкции по настройке и администрированию продукта.
- Руководство специалиста по безопасности — содержит сценарии использования продукта для управления событиями информационной безопасности.
- Руководство пользователя — содержит инструкции по отправке файлов на проверку через интерфейс продукта или по электронной почте и просмотру результатов проверки.
- Руководство разработчика — содержит информацию для интеграции PT Email Security со сторонними системами.

В этом разделе

[Условные обозначения \(см. раздел 1.1\)](#)

[Другие источники информации о PT Email Security \(см. раздел 1.2\)](#)

1.1. Условные обозначения

В документе приняты условные обозначения.

Таблица 1. Условные обозначения

Пример	Описание
Внимание! При выключении модуля снижается уровень защищенности сети	Предупреждения. Содержат информацию о действиях или событиях, которые могут иметь нежелательные последствия
Примечание. Вы можете создать дополнительные отчеты	Примечания. Содержат советы, описания важных частных случаев, дополнительную или справочную информацию, которая может быть полезна при работе с продуктом
► Чтобы открыть файл:	Начало инструкции выделено специальным значком
Нажмите ОК	Названия элементов интерфейса (например, кнопок, полей, пунктов меню) выделены полужирным шрифтом

Пример	Описание
Выполните команду <code>Stop-Service</code>	Текст командной строки, примеры кода, прочие данные, которые нужно ввести с клавиатуры, выделены специальным шрифтом. Также выделены специальным шрифтом имена файлов и пути к файлам и папкам
<code>Ctrl+Alt+Delete</code>	Комбинация клавиш. Чтобы использовать комбинацию, клавиши нужно нажимать одновременно
<Название программы>	Переменные заключены в угловые скобки

1.2. Другие источники информации о PT Email Security

Вы можете найти дополнительную информацию о PT Email Security [на портале технической поддержки](#).

Портал содержит статьи базы знаний, новости обновлений продуктов Positive Technologies, ответы на часто задаваемые вопросы пользователей. Для доступа к базе знаний и всем новостям нужно создать на портале учетную запись.

Если вы не нашли нужную информацию или решение проблемы самостоятельно, обратитесь [в службу технической поддержки \(см. раздел 10\)](#).

2. О PT Email Security

Positive Technologies Email Security (PT Email Security) — система многоуровневой защиты от угроз электронной почты с функциями почтового шлюза и почтового транспортного агента. В системе применяются различные средства статического и динамического анализа объектов, включая антифишинг- и антиспам-проверку, антивирусное сканирование, репутационный, ретроспективный и поведенческий анализ.

PT Email Security предназначен для выявления вредоносных объектов, предотвращения их проникновения и распространения в IT-инфраструктуре организации. Многоуровневая проверка позволяет повысить вероятность обнаружения объектов с угрозами.

PT Email Security может использоваться специалистами по информационной безопасности, администраторами и аналитиками SOC для анализа подозрительных объектов и расследования инцидентов информационной безопасности.

PT Email Security предоставляет следующие основные возможности:

- Инструменты для работы с письмами:
 - Почтовый шлюз безопасности с фильтрацией подключений.
 - Встроенный почтовый транспортный агент.
 - Обработка писем в зависимости от отправителя и получателей.
 - Обезвреживание писем с угрозами.
 - Карантин для подозрительных писем.
- Многоуровневая проверка объектов с использованием методов статического и динамического анализа:
 - Поведенческий анализ файлов в различных операционных системах.
 - Антивирусная проверка файлов.
 - Проверка файлов по YARA-правилам, разработанным специалистами экспертного центра Positive Technologies.
 - Проверка файлов и ссылок по индикаторам компрометации.
 - Антифишинг- и антиспам-проверка писем.
 - Проверка адресов в письмах по спискам DNS-блокировок.
 - Ретроспективный анализ файлов в хранилище.
- Настраиваемые пользователем средства проверки:
 - Черный и белый списки файлов.
 - Проверка файлов по пользовательским YARA-правилам.
 - Пользовательские правила определения файлов и ссылок с угрозами.

- Экспертные инструменты для проверки объектов и расследования инцидентов:
 - Гибкий поиск заданий и объектов с использованием языка запросов QL.
 - Проверка объектов по базам VirusTotal и PT IoC Portal.
 - Поведенческий анализ файлов в интерактивном режиме.
 - Диаграммы поведенческого анализа.
- Быстрая проверка объектов через веб-интерфейс или по электронной почте.
- Поточковая проверка объектов, поступающих из различных источников:
 - Почтовый трафик серверов электронной почты с возможностью блокировки писем с угрозами.
 - Объекты от ICAP-клиентов с возможностью блокировки объектов с угрозами.
 - Объекты из файловых хранилищ и файловых шлюзов.
 - Объекты, передаваемые через публичный API PT Email Security.
- Интеграция с продуктами Positive Technologies:
 - MaxPatrol EDR.
 - MaxPatrol SIEM.
 - PT AF.
 - PT ISIM.
 - PT NAD.
 - PT NGFW.
 - PT Threat Analyzer.

PT Email Security также предоставляет дополнительные возможности:

- Мониторинг проверки объектов и обнаруженных угроз.
- Отправка почтовых уведомлений об угрозах.
- Управление очередью файлов, направляемых на поведенческий анализ.
- Управление приоритетами источников и типов файлов при поведенческом анализе.
- Формирование отчетов по заданиям и проверенным объектам.
- Скачивание проверенных файлов из хранилища.
- Мониторинг работы PT Email Security в Grafana с возможностью отправки почтовых уведомлений.

3. Выбор конфигурации PT Email Security

Предусмотрены несколько конфигураций для развертывания PT Email Security:

- **Базовая конфигурация.** Используется, если аппаратных ресурсов одного узла достаточно для проверки файлов со скоростью, приемлемой для службы информационной безопасности организации. Базовая конфигурация PT Email Security (All-in-One) состоит из одного основного узла с функцией поведенческого анализа.

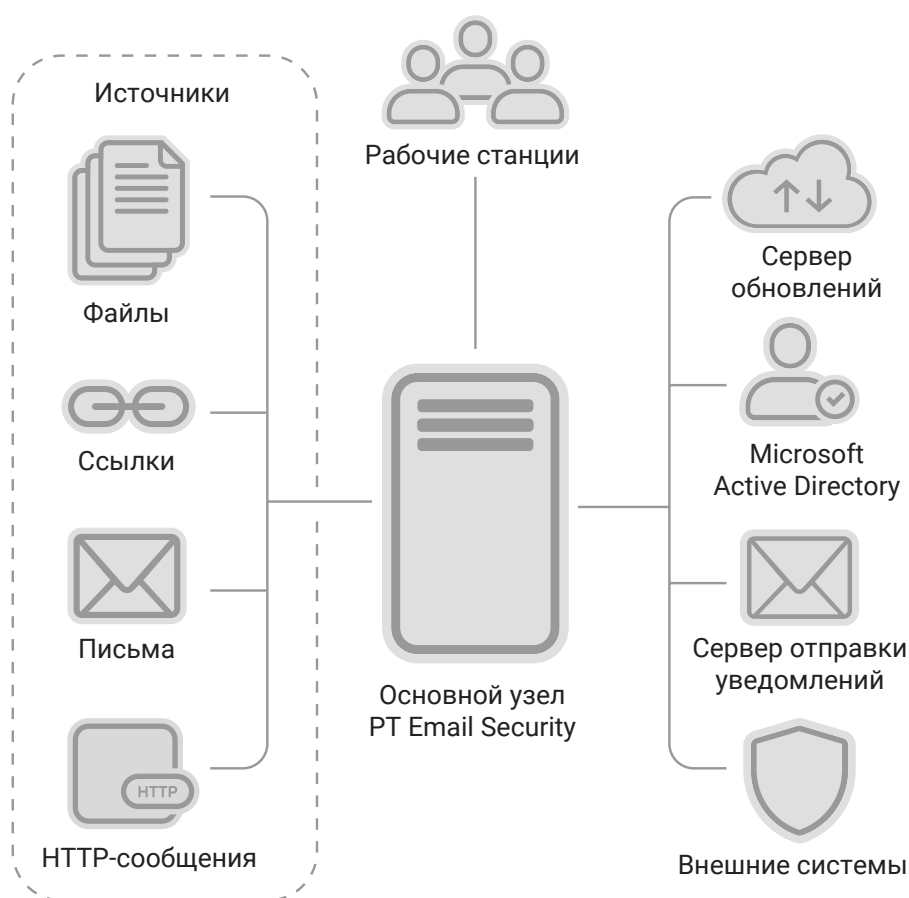


Рисунок 1. Базовая конфигурация PT Email Security

- **Высоконагруженная конфигурация.** Используется, если необходимо увеличить скорость проверки файлов методом поведенческого анализа. Задания на поведенческий анализ распределяются между несколькими специально выделенными для этого дополнительными узлами. Высоконагруженная конфигурация PT Email Security состоит из основного узла (без функции поведенческого анализа) и одного или нескольких дополнительных узлов для поведенческого анализа файлов.



Рисунок 2. Высоконагруженная конфигурация PT Email Security

- **Отказоустойчивый кластер для высоконагруженной конфигурации.** Используется, если необходимо обеспечить бесперебойную работу PT Email Security при высокой скорости проверки файлов. Отказоустойчивый кластер для высоконагруженной конфигурации состоит из основного узла (без функции поведенческого анализа), двух резервных узлов и одного или нескольких дополнительных узлов для поведенческого анализа файлов.

Примечание. Использование отказоустойчивого кластера для географического резервирования не поддерживается.

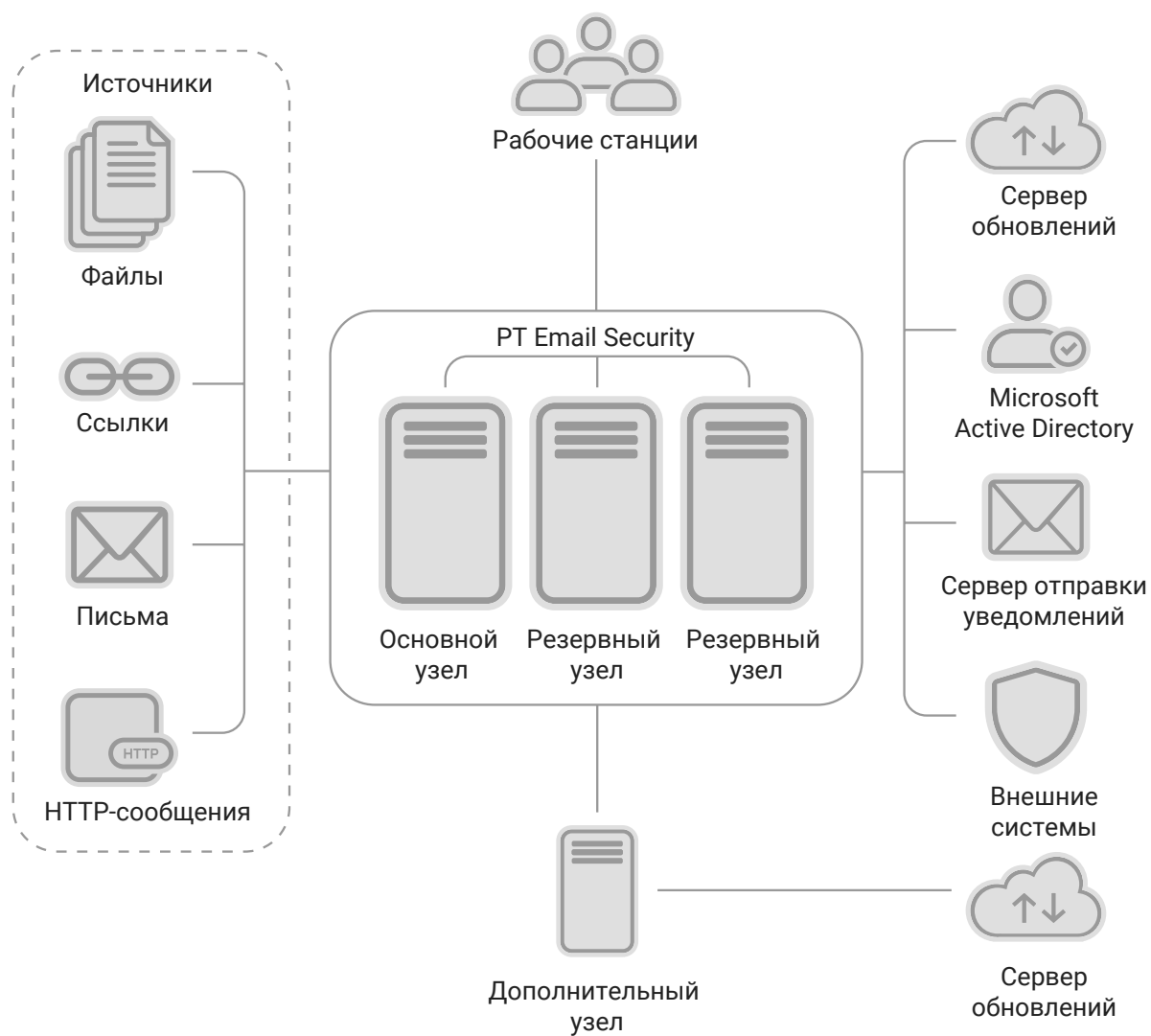


Рисунок 3. Отказоустойчивый кластер для высоконагруженной конфигурации PT Email Security

4. Выбор лицензии PT Email Security

Чтобы использовать PT Email Security, вам нужно приобрести и активировать лицензию. Для приобретения лицензии или изменения параметров уже приобретенной лицензии вы можете обратиться в техническую поддержку Positive Technologies. Лицензия может быть бессрочной или с ограниченным сроком действия. Приобретенная лицензия определяет:

- доступную конфигурацию PT Email Security (включая информацию о допустимом количестве дополнительных узлов и их типах);
- доступные образы виртуальных машин.

Примечание. Одна лицензия может быть активирована только на одном экземпляре PT Email Security.

Бессрочная лицензия

При покупке такой лицензии дополнительно определяется период предоставления обновлений. В рамках лицензии вы можете использовать все функции PT Email Security неограниченное время, в том числе проверять объекты средствами проверки Positive Technologies и методом поведенческого анализа. После окончания периода предоставления обновлений прекратится обновление PT Email Security, образов виртуальных машин, средств проверки Positive Technologies и их баз знаний, но сохранится возможность использования уже установленных версий. Сроки работы и обновления антивирусов определяются их лицензиями.

Лицензия с ограниченным сроком действия

При покупке такой лицензии дополнительно определяются срок ее действия и льготный период. В рамках лицензии вы можете использовать все функции PT Email Security на протяжении всего срока действия лицензии. Сразу после окончания этого срока наступает льготный период, который предназначен для приобретения новой лицензии. В течение льготного периода также работают все функции PT Email Security. Во время срока действия лицензии и льготного периода выполняется обновление PT Email Security, образов виртуальных машин, средств проверки Positive Technologies и их баз знаний. После окончания льготного периода проверка объектов и обновления будут недоступны. Сроки работы и обновления антивирусов определяются их лицензиями.

5. Требования к узлам PT Email Security

В разделе указаны аппаратные и программные требования к узлам для развертывания PT Email Security, а также требования к сетевой инфраструктуре. Количество узлов, а также выдвигаемые к ним аппаратные и программные требования зависят от выбранной вами конфигурации PT Email Security. Узлы PT Email Security могут быть развернуты как на физических серверах, так и в виртуальной среде.

Внимание! Не рекомендуется устанавливать узлы с функцией поведенческого анализа в виртуальной среде.

В этом разделе

[Аппаратные требования \(см. раздел 5.1\)](#)

[Программные требования \(см. раздел 5.2\)](#)

[Требования к сетевой инфраструктуре \(см. раздел 5.3\)](#)

5.1. Аппаратные требования

Аппаратные требования к узлам для развертывания PT Email Security зависят от планируемой нагрузки, от количества одновременно работающих виртуальных машин для поведенческого анализа файлов и от планируемого объема хранилища файлов.

Внимание! Установка узлов PT Email Security с функцией поведенческого анализа возможна только на серверах с центральным процессором Intel, поддерживающим виртуализацию VT-x и технологию расширенных таблиц страниц (EPT). Рекомендуется использовать процессоры на основе Haswell или с более современной микроархитектурой.

Внимание! При установке узлов PT Email Security с функцией поведенческого анализа в операционной системе Debian возможно возникновение ошибок совместимости с SSD-накопителями Intel серии DC P4510.

Внимание! При установке PT Email Security на узлы с сетевыми адаптерами Emulex Corporation серии OneConnect (Skyhawk) рекомендуется использовать операционную систему на базе ядра Linux версии 5. При использовании операционной системой на базе ядра Linux версии 6 могут возникать проблемы с сетевыми подключениями из-за ошибок совместимости.

Основной узел с функцией поведенческого анализа

В таблице указаны минимальные аппаратные требования к физическому серверу для развертывания основного узла PT Email Security с функцией поведенческого анализа в зависимости от количества одновременно создаваемых для поведенческого анализа виртуальных машин. На основном узле одновременно может создаваться не более 15 виртуальных машин.

Примечание. Если на узле установлена защищенная операционная система Astra Linux Special Edition, при тех же аппаратных ресурсах стабильная работа PT Email Security возможна при меньшем количестве одновременно созданных виртуальных машин, чем на узлах с другими поддерживаемыми ОС.

Минимальные размеры дисков в таблице указаны для случая, когда для поведенческого анализа используются только два образа виртуальных машин. При использовании каждого дополнительного образа необходимо увеличить размер SSD на 15 ГиБ (17 ГБ) и размер HDD на 8 ГиБ (9 ГБ).

Вы можете самостоятельно рассчитать минимальные аппаратные требования для основного узла с функцией поведенческого анализа в зависимости от количества виртуальных машин $N_{\text{ВМ}}$ и количества используемых образов виртуальных машин $N_{\text{обр}}$:

- Количество потоков центрального процессора — по формуле $N_{\text{П}} = 3 N_{\text{ВМ}} + 9$.
- Размер памяти ОЗУ — по формуле $V_{\text{ОЗУ}} = 6 N_{\text{ВМ}} + 19$.
- Минимальный размер SSD — по формуле $V_{\text{SSD}} = 2 N_{\text{ВМ}} + 15 N_{\text{обр}} + 161$.
- Минимальный размер HDD — по формуле $V_{\text{HDD}} = 8 N_{\text{обр}} + 50$.

При расчете размера памяти ОЗУ и диска SSD вы получите их размер в ГиБ. Для перевода в ГБ умножьте их на 1,074. К полученному размеру дисков в ГБ рекомендуется прибавить не менее 8% для работы файловой системы.

Таблица 2. Минимальные аппаратные требования для основного узла с функцией поведенческого анализа

Параметр	Количество виртуальных машин		
	2	7	15
Центральный процессор 2,2 ГГц, количество потоков	15	30	54
Память ОЗУ, ГБ	34	66	117
SSD для ОС и компонентов PT Email Security, ГБ	227	238	257
HDD для хранилища файлов, ГБ	77	1100	1100

Основной или резервный узел без функции поведенческого анализа

В таблице указаны минимальные аппаратные требования к физическому серверу для развертывания основного и резервных узлов PT Email Security без функции поведенческого анализа в зависимости от планируемого количества создаваемых за час заданий на проверку

объектов. При этом учтено потребление аппаратных ресурсов на получение объектов, на создание и обработку указанного количества заданий, а также на проверку объектов с помощью доступных средств проверки Positive Technologies и антивирусов.

Примечание. При оценке аппаратных требований учтено, что набор поступающих на проверку объектов зависит от типа источника. Если источником файлов выступает сетевой трафик, набор обычно содержит следующие типы файлов: 60% — документы (DOC, DOCX, ODT, ODS, PDF, XLS), 20% — исполняемые файлы (EXE), 15% — графические файлы (PNG, JPG) и 5% — архивы (ZIP, RAR, 7Z). Для почтовых серверов набор содержит письма с вложенными файлами следующих типов: 40% — графические файлы, 35% — документы, 15% — исполняемые файлы и 10% — архивы.

Таблица 3. Минимальные аппаратные требования для основного и резервных узлов без функции поведенческого анализа

Параметр	Нагрузка (заданий/час)				
	100	1 000	5 000	10 000	100 000
Центральный процессор 2,2 ГГц, количество потоков	4	6	10	15	48
Память ОЗУ, ГБ	16	32	32	32	64
SSD для ОС и компонентов PT Email Security, ГБ	227	227	227	227	227
HDD для хранилища файлов, ГБ	77	1100	1100	1100	1100

Дополнительный узел

В таблице указаны минимальные аппаратные требования к физическому серверу для развертывания дополнительного узла PT Email Security с функцией поведенческого анализа в зависимости от количества одновременно создаваемых для поведенческого анализа виртуальных машин. На одном дополнительном узле одновременно может создаваться не более 45 виртуальных машин.

Внимание! Производительность зависит не только от характеристик процессора, объема ОЗУ и SSD, но и от параметров оборудования (серия процессора, шины данных, тип ОЗУ) и текущей нагрузки (объем, тип и количество объектов). Расчеты минимальных аппаратных требований рекомендуется корректировать на основе данных реальной эксплуатации.

Внимание! Если для поведенческого анализа файлов на узле используется образ с защищенной операционной системой Astra Linux Special Edition, максимальное количество одновременно создаваемых виртуальных машин на узле не должно превышать 30.

Примечание. Если на узле установлена защищенная операционная система Astra Linux Special Edition, при тех же аппаратных ресурсах стабильная работа PT Email Security возможна при меньшем количестве одновременно созданных виртуальных машин, чем на узлах с другими поддерживаемыми ОС.

Минимальный размер диска в таблице рассчитан для случая, когда для поведенческого анализа используются только два образа виртуальных машин. При использовании каждого дополнительного образа необходимо увеличить размер SSD на 15 ГиБ (17 ГБ).

Вы можете самостоятельно рассчитать минимальные аппаратные требования для дополнительного узла в зависимости от количества виртуальных машин $N_{\text{ВМ}}$ и количества используемых образов виртуальных машин $N_{\text{обр}}$:

- Количество потоков центрального процессора:
 - Если $N_{\text{ВМ}} < 10$ — по формуле $N_{\text{П}} = 3 N_{\text{ВМ}} + 4$.
 - Если $N_{\text{ВМ}} \geq 10$ — по формуле $N_{\text{П}} = 2 N_{\text{ВМ}} + 14$.
- Размер памяти ОЗУ:
 - Если $N_{\text{ВМ}} \leq 15$ — по формуле $V_{\text{ОЗУ}} = 6 N_{\text{ВМ}} + 5$.
 - Если $N_{\text{ВМ}} > 15$ — по формуле $V_{\text{ОЗУ}} = 6,4 N_{\text{ВМ}} + 4$.
- Минимальный размер SSD — по формуле $V_{\text{SSD}} = 2 N_{\text{ВМ}} + 15 N_{\text{обр}} + 116$.

При расчете размера памяти ОЗУ и диска SSD вы получите их размер в ГиБ. Для перевода в ГБ умножьте его на 1,074. К полученному размеру SSD в ГБ рекомендуется прибавить не менее 8% для работы файловой системы.

Таблица 4. Минимальные аппаратные требования для дополнительного узла

Параметр	Количество ВМ			
	2	15	30	45
Центральный процессор 2,2 ГГц, количество потоков	10	44	74	104
Память ОЗУ, ГБ	19	102	211	314
SSD для ОС и компонентов PT Email Security, ГБ	175	205	240	274

Примеры аппаратных конфигураций

В таблице приведены примеры аппаратных конфигураций для основного узла с функцией поведенческого анализа и для дополнительного узла.

Таблица 5. Примеры аппаратных конфигураций

Параметр	Основной узел с функцией поведенческого анализа	Дополнительный узел
Центральный процессор		
Количество	2 × Intel Xeon Gold 6230R	
Частота	2,1 ГГц	
Потоки	2 × 52	
Память ОЗУ		
Объем	256 ГБ	384 ГБ
Твердотельные накопители (SSD)		
Количество и объем	4 × 960 ГБ	
Интерфейс	SAS	
Уровень RAID	RAID 5 или RAID 10	
Тип	Mixed Use	
Жесткие диски (HDD)		
Количество и объем	6 × 8 ТБ	—
Скорость	7200 об/мин	—
Интерфейс	NL SAS	—
Уровень RAID	RAID 5 или RAID 10	—
Сетевые платы		
Количество и скорость сетевых портов для доступа к веб-интерфейсу	2 × 1 Гбит/с, 2 × 10 Гбит/с	

5.2. Программные требования

К узлам для развертывания PT Email Security выдвигаются следующие общие требования:

- Для узлов настроены статические IP-адреса.
- Узлам присвоены уникальные имена (hostnames) в рамках конфигурации PT Email Security.
- С узлов обеспечен доступ к серверам обслуживания Positive Technologies по протоколу HTTPS.

К настройке операционных систем на узлах PT Email Security выдвигаются следующие требования:

- Установлено точное время и настроена синхронизация с NTP-сервером.
- Настроено подключение к DNS-серверу.

Примечание. Файл `/etc/hosts` не используется компонентами PT Email Security, поэтому не рекомендуется вносить изменения в этот файл.

- Не используется прокси-сервер на уровне операционной системы.
- Отсутствуют антивирусы, работающие отдельно от PT Email Security.

В этом разделе

[Требования к настройке BIOS и UEFI \(см. раздел 5.2.1\)](#)

[Требования к разметке жесткого диска \(см. раздел 5.2.2\)](#)

[Требования к ОС для развертывания с помощью установщика \(см. раздел 5.2.3\)](#)

[Особенности развертывания в виртуальной среде \(см. раздел 5.2.4\)](#)

5.2.1. Требования к настройке BIOS и UEFI

На узлах для развертывания PT Email Security выдвигаются следующие требования к настройке BIOS и UEFI:

- Отключено энергосбережение для центрального процессора.
- Отключено динамическое управление частотой центрального процессора.
- На узлах с функцией поведенческого анализа включена аппаратная поддержка виртуализации.
- На узлах с функцией поведенческого анализа отключена функция Secure Boot.

Таблица 6. Пример настройки параметров процессора серии Intel Xeon Scalable в BIOS AMI

Параметр	Значение		Примечание
	По умолчанию	Требуемое	
Intel SpeedStep Technology	Enabled	Disabled	Отключено изменение частоты
Long Duration Power Limit	>0	0	Сняты ограничения по энергопотреблению
Intel Virtualization Technology	Enabled	Enabled	Включена аппаратная поддержка виртуализации (для узлов с функцией поведенческого анализа)

Параметр	Значение		Примечание
	По умолчанию	Требуемое	
Package C State Support	C0/C1 state	C0/C1 state	Выбран базовый режим простоя без глубоких состояний
CPU C6 State Support	Enabled	Disabled	Отключено глубокое энергосбережение (C6)
Enhanced Halt State (C1E)	Enabled	Disabled	Отключено расширенное состояние простоя (C1E)
Hardware P-States	Enabled	Disabled	Отключено динамическое управление частотой
Secure Boot	Enabled	Disabled	Отключена проверка цифровых подписей компонентов при загрузке (для узлов с функцией поведенческого анализа)

5.2.2. Требования к разметке жесткого диска

При установке операционной системы на узлах PT Email Security необходимо разметить дисковое пространство. В таблицах ниже указаны размеры разделов для файлов операционной системы, программных модулей PT Email Security, хранилища файлов заданий и пользовательских данных.

Внимание! Разделы для системных файлов и программных модулей PT Email Security рекомендуется создавать на твердотельном накопителе, а разделы для хранилища файлов и пользовательских данных — на жестком диске.

В таблицах ниже указаны минимальные размеры разделов в зависимости от количества создаваемых для поведенческого анализа виртуальных машин и рекомендованные размеры разделов. Минимальные требования рассчитаны для работы PT Email Security под низкой нагрузкой, когда за час создается не более ста заданий на проверку объектов.

Основной узел с функцией поведенческого анализа

В таблице указаны размеры разделов дисков на основном узле PT Email Security с функцией поведенческого анализа. На основном узле одновременно может создаваться не более 15 виртуальных машин.

Минимальные размеры разделов в таблице указаны для случая, когда для поведенческого анализа используются только два образа виртуальных машин. При использовании каждого дополнительного образа необходимо увеличить размер раздела для программных модулей PT Email Security на 15 ГиБ (17 ГБ) и раздела для хранилища файлов — на 8 ГиБ (9 ГБ).

Вы можете самостоятельно рассчитать минимальные размеры разделов на основном узле с функцией поведенческого анализа в зависимости от количества виртуальных машин $N_{\text{ВМ}}$ и количества используемых образов виртуальных машин $N_{\text{обр}}$:

- Размер раздела для файлов операционной системы — по формуле $V = N_{\text{ВМ}} + 118$.
- Размер раздела для программных модулей PT Email Security — по формуле $V_{\text{opt}} = N_{\text{ВМ}} + 15 N_{\text{обр}} + 43$.
- Размер раздела для хранилища файлов — по формуле $V_{\text{minio}} = 8 N_{\text{обр}} + 50$.

Вы получите размеры разделов в ГиБ. Для перевода в ГБ умножьте их на 1,074. При разметке диска полученные размеры разделов в ГБ рекомендуется увеличить на 8% или более для работы файловой системы.

Таблица 7. Разметка диска на основном узле с функцией поведенческого анализа

Тип данных	Точка монтирования	Размер ¹ , ГиБ / ГБ			
		Минимальный (по количеству ВМ)			Рекомендуемый
		2	7	15	
Системные файлы	/	120 / 140	125 / 145	133 / 155	220 / 240
Программные модули PT Email Security	/opt	75 / 87	80 / 93	88 / 102	900 / 1000
Хранилище файлов	/opt/ ptms/var/ minio	66 / 77	66 / 77	66 / 77	От 900 / 1000
Пользовательские	/home	—	—	—	От 90 / 100

Основной или резервный узел без функции поведенческого анализа

В таблице указаны размеры разделов дисков на основном и резервных узлах PT Email Security без функции поведенческого анализа.

Минимальный размер раздела для хранилища файлов в таблице рассчитан для случая, когда для поведенческого анализа используются только два образа виртуальных машин. При использовании каждого дополнительного образа необходимо увеличить размер раздела на 8 ГиБ (9 ГБ).

¹ Первое значение — размер файловой системы в ГиБ. Этот размер проверяется при установке компонентов PT Email Security. Второе значение — размер раздела диска в ГБ. На этот размер вы можете ориентироваться при разметке диска.

Размеры разделов для файлов операционной системы и программных модулей PT Email Security на основном и резервных узлах без функции поведенческого анализа не зависят от количества виртуальных машин и образов. Вы можете самостоятельно рассчитать минимальный размер раздела для хранилища файлов в зависимости от количества образов $N_{обр}$ по формуле $V_{minio} = 8 N_{обр} + 50$. Вы получите размер раздела в ГиБ. Для перевода в ГБ умножьте его на 1,074. При разметке диска полученный размер раздела в ГБ рекомендуется увеличить на 8% или более для работы файловой системы.

Таблица 8. Разметка диска на основном и резервных узлах без функции поведенческого анализа

Тип данных	Точка монтирования	Размер ¹ , ГиБ / ГБ	
		Минимальный	Рекомендуемый
Системные файлы	/	120 / 140	220 / 240
Программные модули PT Email Security	/opt	75 / 87	900 / 1000
Хранилище файлов	/opt/ptms/var/minio	66 / 77	От 900 / 1000
Пользовательские	/home	—	От 90 / 100

Дополнительный узел с функцией поведенческого анализа

В таблице указаны размеры разделов диска на дополнительном узле PT Email Security с функцией поведенческого анализа. На одном дополнительном узле одновременно может создаваться не более 30 виртуальных машин.

Минимальный размер раздела для программных модулей PT Email Security в таблице рассчитан для случая, когда для поведенческого анализа используются только два образа виртуальных машин. При использовании каждого дополнительного образа необходимо увеличить размер раздела на 15 ГиБ (17 ГБ).

Вы можете самостоятельно рассчитать минимальные размеры разделов на дополнительном узле с функцией поведенческого анализа в зависимости от количества виртуальных машин $N_{ВМ}$ и количества используемых образов виртуальных машин $N_{обр}$:

- Размер раздела для файлов операционной системы — по формуле $V = N_{ВМ} + 118$.
- Размер раздела для программных модулей PT Email Security — по формуле $V_{opt} = N_{ВМ} + 15 N_{обр} - 2$.

Вы получите размер раздела в ГиБ. Для перевода в ГБ умножьте его на 1,074. При разметке диска полученные размеры разделов в ГБ рекомендуется увеличить на 8% или более для работы файловой системы.

Таблица 9. Разметка диска на дополнительном узле с функцией поведенческого анализа

Тип данных	Точка монтирования	Размер ¹ , ГиБ / ГБ				Рекомендуемый
		Минимальный (по количеству ВМ)				
		2	15	30	45	
Системные файлы	/	120 / 140	133 / 155	148 / 172	163 / 189	220 / 240
Программные модули PT Email Security	/opt	30 / 35	43 / 50	58 / 68	73 / 85	900 / 1000
Пользовательские	/home	—	—	—	—	От 90 / 100

5.2.3. Требования к ОС для развертывания с помощью установщика

Установка PT Email Security с помощью установщика возможна на узлах с 64-разрядной операционной системой:

- Astra Linux Special Edition версий 1.7, 1.8 (уровень защищенности «Смоленск»);
- Debian GNU/Linux версий 12;
- «ОСнова» версии 2.11 (Onyx).

При установке операционной системы рекомендуется выбирать наиболее актуальную версию ядра Linux из доступных в дистрибутиве.

К настройке операционных систем на узлах для развертывания PT Email Security выдвигаются следующие требования:

- Отсутствует раздел или файла подкачки.
- Установлена программа sudo. Пользователь, от имени которого выполняется установка, добавлен в группу sudo.
- Настроен менеджер пакетов APT с корректным индексом пакетов (используется при установке и обновлении PT Email Security).

Примечание. Вы можете проверить корректность индексов пакетов, запустив на узле команду `sudo apt-get check`.

Особенности развертывания на узлах с Astra Linux

Внимание! При установке операционной системы Astra Linux в окне **Дополнительные настройки ОС** должны быть сняты флажки **Мандатный контроль целостности** и **Мандатное управление доступом**.

Подсистемы безопасности Astra Linux, в частности `auditd` — служба регистрации событий безопасности, могут влиять на производительность PT Email Security. Вы можете повысить производительность PT Email Security, настроив или отключив службу `auditd` и перезагрузив ОС.

Внимание! Полное отключение службы `auditd` может повлиять на функцию аудита в ОС. Изменяйте параметры службы `auditd` или отключайте ее в Astra Linux только в том случае, если это допускается сертификационными требованиями и политиками безопасности вашей организации.

Особенности развертывания на узлах с «ОСнова»

К операционной системе «ОСнова» выдвигаются следующие дополнительные требования:

- Должен быть отключен механизм защиты памяти `Rax MPROTECT`.

Примечание. Для отключения механизма защиты памяти вы можете в файле `/etc/default/grub` в строке `GRUB_CMDLINE_LINUX_DEFAULT` указать значение `mprotect=off`. После этого необходимо обновить конфигурацию загрузчика `sudo update-grub` и перезагрузить операционную систему `sudo reboot`.

- Должен быть отключен пароль загрузчика операционной системы.

Примечание. Для отключения пароля загрузчика вы можете выполнить команду `sudo rm -rf /etc/grub.d/07_password`. После этого необходимо обновить конфигурацию загрузчика `sudo update-grub` и перезагрузить операционную систему `sudo reboot`.

5.2.4. Особенности развертывания в виртуальной среде

Для установки узлов PT Email Security в виртуальной среде необходимо использовать гипервизор VMware ESXi версии 6.0 или выше с аппаратным обеспечением версии 11 или выше.

Внимание! Не рекомендуется устанавливать узлы с функцией поведенческого анализа в виртуальной среде. Использование вложенной виртуализации (*nested virtualization*) может привести к значительному снижению производительности PT Email Security.

Внимание! Базовая конфигурация (All-in-One) не поддерживается при установке PT Email Security в виртуальной среде. Для поведенческого анализа файлов должен быть выделен отдельный дополнительный узел.

При установке узлов PT Email Security в виртуальной среде:

- Не поддерживается использование снапшотов. Восстановление состояния гостевой ОС из снапшота может привести к неработоспособности узла.
- Не поддерживается использование дисков с емкостью, выделяемой по требованию (технология *thin provisioning*).

При установке узлов PT Email Security с функцией поведенческого анализа в виртуальной среде:

- Для гостевой ОС должна быть включена аппаратная поддержка виртуализации.
- Если узел запускается при помощи UEFI, в его параметрах должна быть отключена функция Secure Boot.

5.3. Требования к сетевой инфраструктуре

На рабочей станции, с которой выполняется развертывание PT Email Security, должны быть разрешены исходящие подключения к портам TCP 22, 80, 443, 3334, 8703, 8704.

Внимание! Не рекомендуется назначать публичные IP-адреса сетевым интерфейсам узлов PT Email Security. Для всех интерфейсов необходимо использовать адреса из частных диапазонов (RFC 1918). Также не рекомендуется прямое подключение узлов к интернету. Для доступа к внешним ресурсам следует использовать шлюз с NAT или прокси-сервер.

Порты взаимодействия узлов PT Email Security

Для работы компонентов PT Email Security на узлах должны быть разрешены входящие и исходящие подключения к портам, указанным в таблице.

В PT Email Security используется контейнеризация приложений на основе технологий Kubernetes. В рамках кластера Kubernetes используется подсеть 10.244.0.0/16 для подов и подсеть 10.96.0.0/24 для служб. Для исключения проблем маршрутизации рекомендуется избегать пересечения адресных пространств внешних систем с этими подсетями.

Таблица 10. Порты взаимодействия узлов PT Email Security

Протокол и порт	Назначение
Внутренние подключения основного и резервных узлов	
TCP 179	Обмен маршрутами BGP при работе плагина Calico
TCP 2379	Доступ API-сервера Kubernetes к хранилищу etcd
TCP 2380	Синхронизация данных в хранилище etcd
TCP 5473	Взаимодействие компонентов Calico с сервером Typha
TCP 6443	Доступ к API-серверу Kubernetes
TCP 9100	Мониторинг системных ресурсов узлов компонентом node-exporter
TCP 10250	Обмен данными между kubelet и управляющими компонентами Kubernetes
UDP 53	Обработка DNS-запросов через CoreDNS
UDP 4789	Передача сетевого трафика через VXLAN

Протокол и порт	Назначение
VRRP	Работа службы Keepalived
Подключения от основного узла к дополнительному	
TCP 179	Обмен маршрутами BGP при работе плагина Calico
TCP 5900—5999	Подключение по VNC при выполнении поведенческого анализа в интерактивном режиме
TCP 9100	Мониторинг системных ресурсов узлов компонентом node-exporter
TCP 10250	Обмен данными между kubelet и управляющими компонентами Kubernetes
UDP 53	Обработка DNS-запросов через CoreDNS
UDP 4789	Передача сетевого трафика через VXLAN
Подключения от дополнительного узла к основному	
TCP 179	Обмен маршрутами BGP при работе плагина Calico
TCP 5473	Взаимодействие компонентов Calico с сервером Typha
TCP 6443	Доступ к API-серверу Kubernetes
TCP 9100	Мониторинг системных ресурсов узлов компонентом node-exporter
UDP 53	Обработка DNS-запросов через CoreDNS
UDP 4789	Передача сетевого трафика через VXLAN
Подключения между дополнительными узлами	
TCP 179	Обмен маршрутами BGP между узлами при работе плагина Calico
TCP 9100	Мониторинг системных ресурсов узлов компонентом node-exporter
TCP 12345	Работа службы анализатора сетевого трафика виртуальных машин
UDP 53	Обработка DNS-запросов через CoreDNS
UDP 4789	Передача сетевого трафика через VXLAN

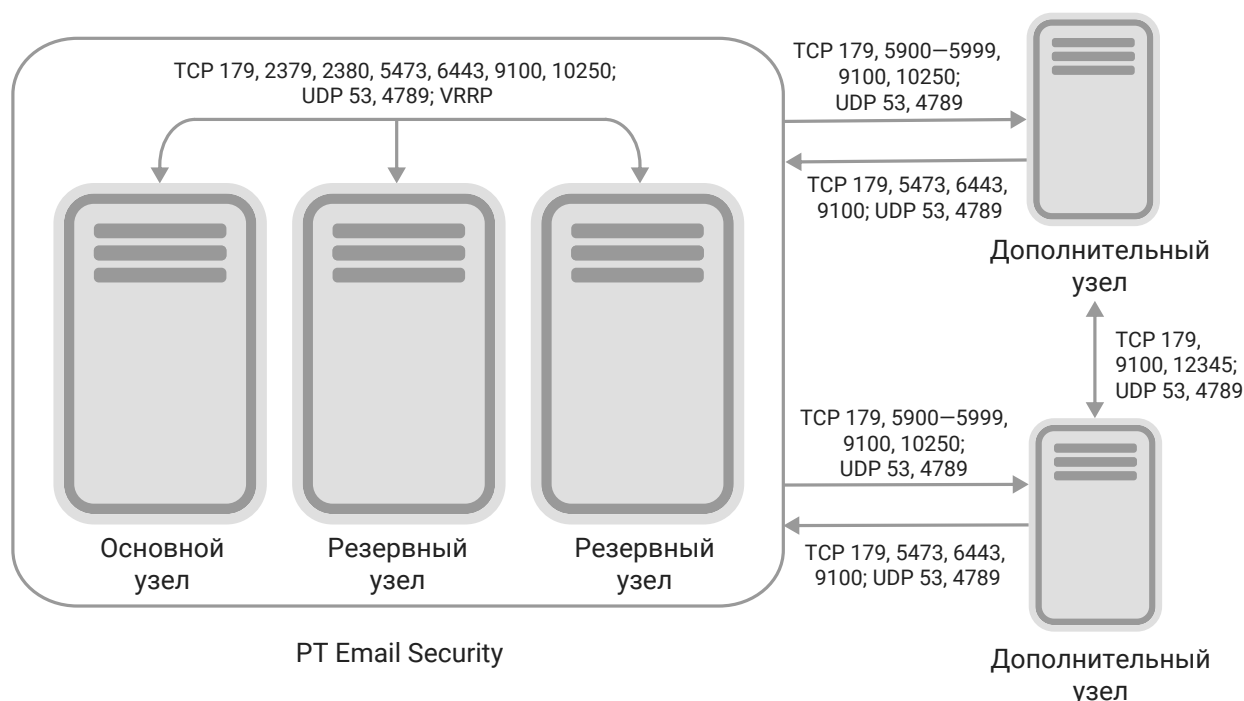


Рисунок 4. Порты взаимодействия узлов PT Email Security

Порты взаимодействия основного и резервных узлов PT Email Security с компонентами информационной системы

Для сетевого взаимодействия PT Email Security с другими компонентами информационной системы на основном и резервных узлах должны быть разрешены входящие и исходящие подключения к портам, указанным в таблице.

Внимание! В конфигурации с отказоустойчивым кластером на основном и резервных узлах должны быть разрешены входящие подключения от других компонентов информационной системы не только по реальным IP-адресам этих узлов, но и по виртуальному IP-адресу кластера.

Таблица 11. Порты взаимодействия основного и резервных узлов с компонентами информационной системы

Компонент	Протокол и порт	Направление подключения	Назначение
Рабочая станция администратора	SSH (TCP 22)	Входящие	Подключение по протоколу SSH для взаимодействия с ОС на узле PT Email Security

Компонент	Протокол и порт	Направление подключений	Назначение
	HTTPS (TCP 80, 443)	Входящие	Доступ к интерфейсу PT Email Security и к сервису публичного API
	HTTPS (TCP 3334, 8703, 8704)	Входящие	Подключение к PT MC для аутентификации
Рабочие станции операторов	HTTPS (TCP 80, 443)	Входящие	Доступ к интерфейсу PT Email Security. Внимание! Если используется обратный прокси-сервер (reverse proxy), на нем должно быть настроено проксирование WebSocket-соединений. Это требуется для выполнения поведенческого анализа файлов в интерактивном режиме
	HTTPS (TCP 3334, 8703, 8704)	Входящие	Подключение к PT MC для аутентификации
Сервер Positive Technologies	HTTPS (TCP 443)	Исходящие	Загрузка обновлений и активация лицензии PT Email Security с сервера update.ptsecurity.com
Сетевые ресурсы	HTTP (TCP) или HTTPS (TCP)	Исходящие	Динамическая проверка ссылок с помощью PT Crawler
Прокси-сервер для проверки ссылок	HTTP (TCP) или HTTPS (TCP)	Исходящие	Динамическая проверка ссылок с помощью PT Crawler через прокси-сервер. Номер порта прокси-сервера задается в параметрах PT Crawler
Внешний PT MC	HTTPS (TCP 3334, 8703, 8704)	Исходящие	Подключение к внешнему PT MC для аутентификации пользователей
Локальный сервер обновлений	HTTP (TCP 8553) или HTTPS (TCP 8743)	Исходящие	Загрузка обновлений PT Email Security

Компонент	Протокол и порт	Направление подключений	Назначение
Сервер обновлений дополнительных антивирусов	HTTP (TCP) или HTTPS (TCP)	Исходящие	Обновление антивирусов. Номер порта зависит от антивируса
Источник объектов, работающий через API	HTTPS (TCP 80, 443)	Входящие	Доступ к интерфейсу и к сервису публичного API
Почтовый сервер для досылки писем из карантина	SMTP (TCP 587, 10025)	Исходящие	Досылка писем из карантина для источников, работающих в блокирующем режиме. Номер порта задается в параметрах источника
Почтовый сервер для отправки уведомлений	SMTP	Исходящие	Отправка уведомлений об обнаружении опасных и потенциально опасных файлов. Номер порта задается в параметрах настройки уведомлений
DNS-сервер	DNS (TCP 53, UDP 53)	Исходящие	Подключение к DNS-серверу
NTP-сервер	UDP 123	Исходящие	Синхронизация времени
Syslog-сервер	SYSLOG (TCP 1468 или UDP 514)	Исходящие	Отправка сообщений стандарта syslog в MaxPatrol SIEM или другие системы для централизованного сбора и анализа событий ИБ. Номер порта и протокол задаются в основных параметрах PT Email Security

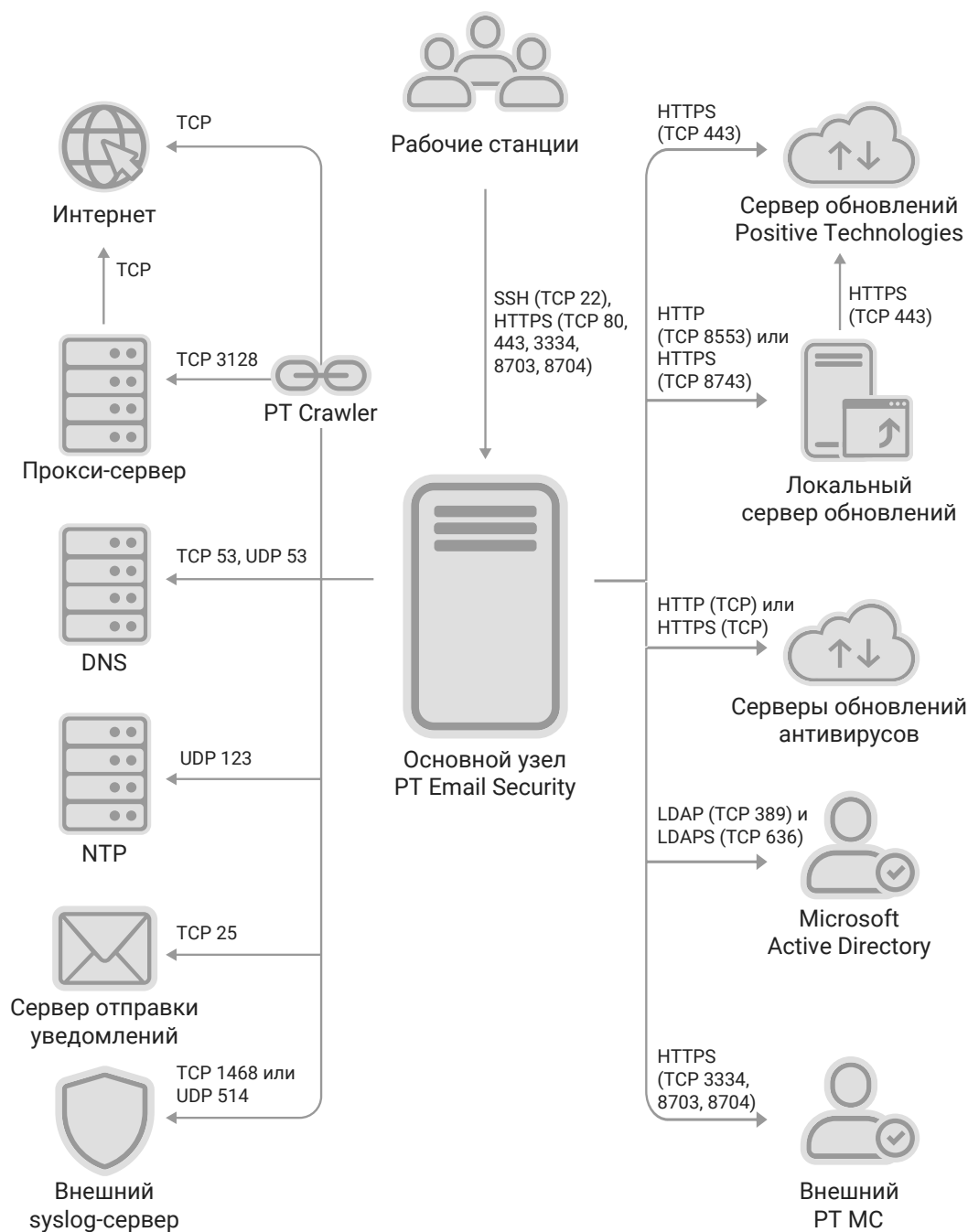


Рисунок 5. Порты взаимодействия основного узла PT Email Security с компонентами информационной системы

Порты взаимодействия дополнительных узлов PT Email Security с компонентами информационной системы

На дополнительных узлах PT Email Security должны быть разрешены входящие и исходящие подключения к портам, указанным в таблице.

В ходе поведенческого анализа компоненты гостевых ОС виртуальных машин и артефакты анализа могут инициировать исходящие подключения к внешним сетевым ресурсам. При этом используются произвольные порты и протоколы. В заголовке *Host* указывается IP-адрес узла, на котором выполняется анализ, а заголовок *User-Agent* формируется в зависимости от компонента ОС или артефакта.

Примечание. При использовании прокси-сервера гостевые ОС виртуальных машин, запускаемых для поведенческого анализа файлов, не имеют доступа к внешним сетевым ресурсам. Для настройки доступа на узле с функцией поведенческого анализа необходимо добавить сетевой интерфейс и настроить маршрутизацию трафика виртуальных машин через отдельный шлюз. За инструкцией вы можете обратиться в техническую поддержку Positive Technologies.

Таблица 12. Порты взаимодействия дополнительных узлов с компонентами информационной системы

Компонент	Протокол и порт	Направление подключений	Назначение
Рабочая станция администратора	SSH (TCP 22)	Входящие	Подключение по протоколу SSH для взаимодействия с ОС узла
Сервер Positive Technologies	HTTPS (TCP 443)	Исходящие	Загрузка обновлений и активация лицензии PT Email Security с сервера update.ptsecurity.com
Локальный сервер обновлений	HTTP (TCP 8553) или HTTPS (TCP 8743)	Исходящие	Обновление PT Email Security
DNS-сервер	DNS (TCP 53, UDP 53)	Исходящие	Подключение к DNS-серверу
NTP-сервер	UDP 123	Исходящие	Синхронизация времени

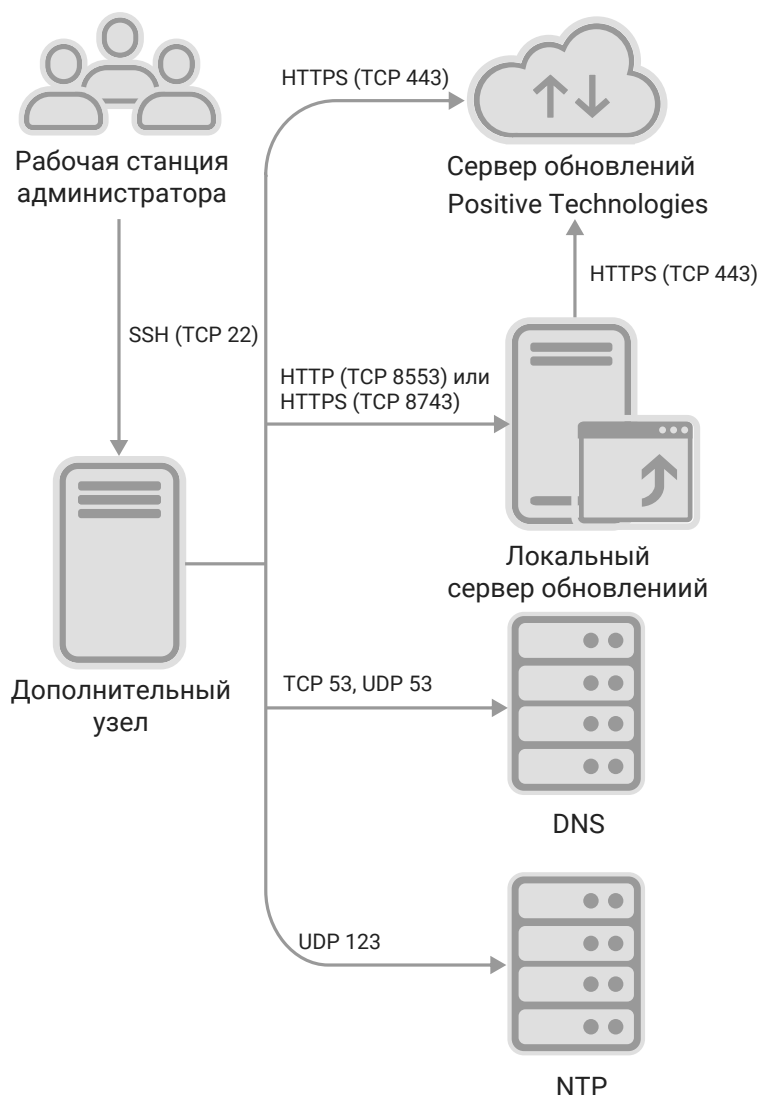


Рисунок 6. Порты взаимодействия дополнительного узла PT Email Security с компонентами информационной системы

Порты взаимодействия PT Email Security с источниками объектов для проверки

Для сетевого взаимодействия PT Email Security с источниками объектов на основном и резервных узлах должны быть разрешены входящие и исходящие подключения к портам, указанным в таблице. Вы можете изменить номер порта в параметрах источника.

Внимание! Порт, указанный в параметрах источника, не должен использоваться другими источниками, службами или приложениями ОС.

Таблица 13. Порты взаимодействия PT Email Security с источниками объектов для проверки

Источник для проверки	Порт и протокол	Направление подключений
Checkme	IMAP (TCP 143, 993), SMTP (TCP 465, 587)	Исходящие
Общая папка и папка-шлюз	NFS (TCP 111, 2049), SMB (TCP 139, 445)	Исходящие
ICAP-сервер	ICAP (TCP 1344)	Входящие
PT NAD	ICAP (TCP 2344)	Входящие
MaxPatrol EDR	HTTPS (TCP 80, 443)	Входящие
Сервер Microsoft Exchange с установленным агентом	TCP 7536	Исходящие
Почтовый сервер в режиме фильтрации	SMTP (TCP 25, 10025)	Входящие, Исходящие
Почтовый сервер в режиме фильтрации (MTA)	SMTP (TCP 25, 10025)	Входящие, Исходящие
Почтовый сервер в режиме зеркалирования	SMTP (TCP 25)	Входящие
Почтовый шлюз безопасности Примечание. На узле почтового шлюза безопасности должны быть разрешены входящие подключения через порт SMTP (TCP 25)	TCP 50052, SMTP (TCP 25)	Входящие
API с выбранными параметрами проверки	HTTPS (TCP 80, 443)	Входящие
API с передаваемыми параметрами проверки	HTTPS (TCP 80, 443)	Входящие

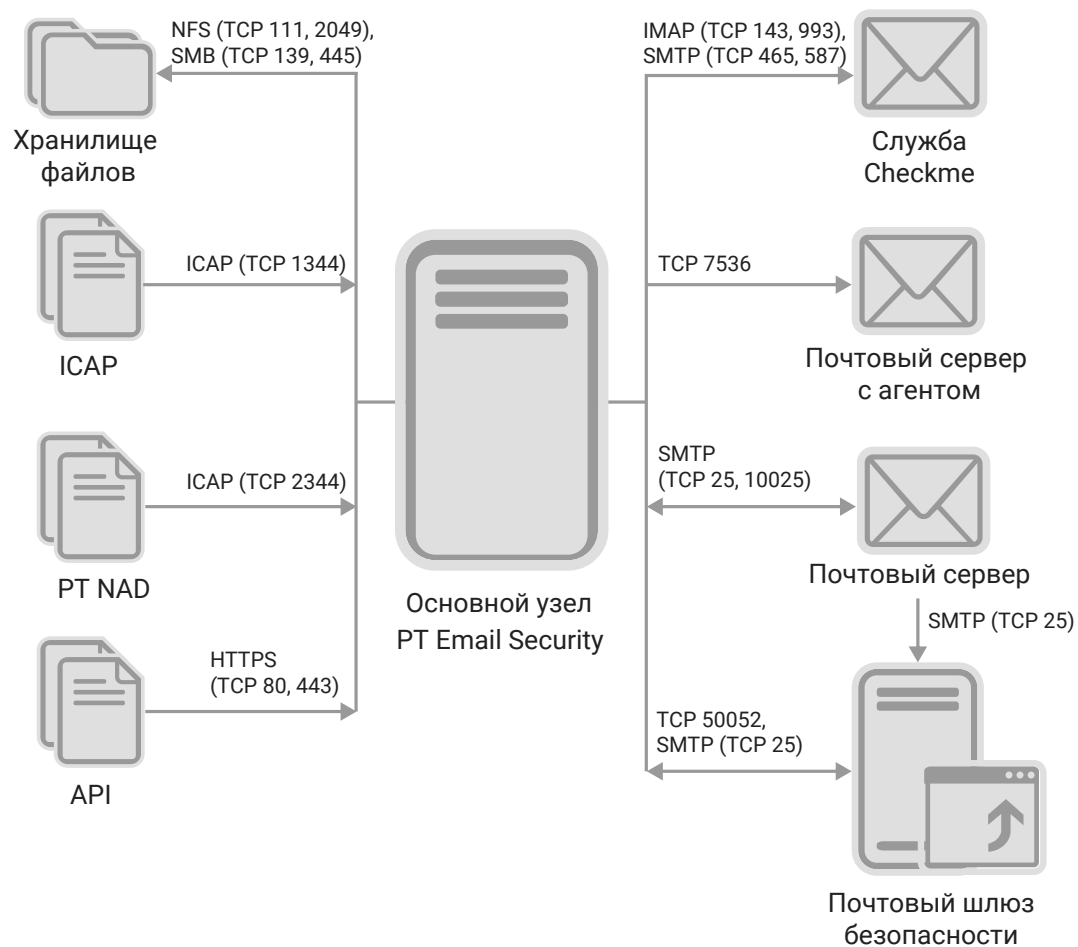


Рисунок 7. Порты взаимодействия PT Email Security с источниками

6. Установка локального сервера обновлений

Если PT Email Security не имеет доступа к внешним ресурсам, для его обновления можно использовать локальный сервер обновлений. Такой сервер может быть установлен в сети организации или в демилитаризованной зоне (DMZ). Обновления могут скачиваться напрямую с сервера обновлений Positive Technologies или через прокси-сервер. Если в вашей организации используется несколько продуктов Positive Technologies, вы можете организовать их обновление через общий локальный сервер обновлений.



Рисунок 8. Обновление PT Email Security через локальный сервер обновлений

Для настройки обновлений PT Email Security через локальный сервер обновлений вам нужно:

1. Установить локальный сервер обновлений.
2. Если для доступа к серверу обновлений Positive Technologies используется прокси-сервер, указать его в параметрах сервера обновлений.
3. Активировать лицензию PT Email Security на локальном сервере обновлений.
4. Указать в PT Email Security локальный сервер в качестве источника обновлений.

Обновление PT Email Security в изолированном сегменте сети

Если PT Email Security установлен в изолированном сегменте сети и не имеет доступа к внешним ресурсам, для его обновления можно использовать два локальных серверов обновлений. Первый сервер устанавливается в изолированном сегменте сети и служит

источником обновлений для PT Email Security. Второй сервер устанавливается в демилитаризованной зоне (DMZ) и предназначен для скачивания обновлений с сервера обновлений Positive Technologies напрямую или через прокси-сервер.



Рисунок 9. Обновление PT Email Security в изолированном сегменте сети

Для настройки обновлений PT Email Security в изолированном сегменте сети вам нужно:

1. Установить локальный сервер обновлений в DMZ.
2. Если для доступа к серверу обновлений Positive Technologies используется прокси-сервер, указать его в параметрах сервера.
3. Активировать лицензию PT Email Security на локальном сервере обновлений в DMZ.
4. Установить второй локальный сервер обновлений в изолированном сегменте сети.
5. Если между этим локальным сервером и сервером обновлений в DMZ есть сетевая связность, активировать на сервере лицензию PT Email Security.
6. Настроить перенос обновлений в изолированный сегмент сети:
 - Если между локальными серверами обновлений есть сетевая связность, вы можете настроить автоматический перенос обновлений.
 - Если сетевой связности нет, вы можете переносить обновления вручную при помощи внешнего носителя.
7. Указать в PT Email Security локальный сервер обновлений в изолированном сегменте сети в качестве источника обновлений.

В этом разделе

[Аппаратные и программные требования \(см. раздел 6.1\)](#)

[Установка локального сервера обновлений \(см. раздел 6.2\)](#)

[Настройка локального сервера обновлений \(см. раздел 6.3\)](#)

[Активация лицензии \(см. раздел 6.4\)](#)

[Перенос обновлений в изолированный сегмент сети \(см. раздел 6.5\)](#)

[Выбор локального сервера в качестве источника обновлений \(см. раздел 6.6\)](#)

6.1. Аппаратные и программные требования

Для обновления PT Email Security требуется локальный сервер обновлений версии 2.0 или выше. Локальный сервер обновлений может быть установлен как на физическом сервере, так и в виртуальной среде.

Для загрузки обновлений и проверки лицензии с узла для установки локального сервера обновлений должен быть обеспечен доступ по протоколу HTTPS к серверу `update.ptsecurity.com`. По умолчанию используется порт TCP 443.

Аппаратные требования

Минимальные аппаратные требования для установки локального сервера обновлений указаны в таблице.

Примечание. Объем свободного места на жестком диске зависит от количества образов VM, используемых в PT Email Security для поведенческого анализа файлов. Вы можете самостоятельно рассчитать необходимый свободный объем в ГБ по формуле $V = 30 N_{\text{обр}} + 200$.

Таблица 14. Минимальные аппаратные требования

Параметр	Количество используемых образов VM		
	2	7	14
Центральный процессор 2,2 ГГц, количество потоков	2	2	2
Память ОЗУ, ГБ	4	4	4
HDD или SSD, ГБ	260	410	620

Программные требования

Установка локального сервера обновлений возможна в 64-разрядных операционных системах Astra Linux 1.7.3, 1.7.4 и Debian GNU/Linux 10, 11, 12.8. Установочные файлы локального сервера обновлений входят в состав установщиков PT Email Security для этих версий операционных систем.

Примечание. Вы также можете установить локальный сервер обновлений в 64-разрядных операционных системах Debian GNU/Linux 9 и Ubuntu 16, 18. Для получения установочных файлов локального сервера обновлений для этих версий операционных систем обратитесь в техническую поддержку Positive Technologies.

К настройке операционной системы на узле для установки локального сервера обновлений выдвигаются следующие требования:

- Установлено точное время и настроена синхронизация с NTP-сервером.
- Настроено подключение к DNS-серверу.
- Настроен менеджер пакетов APT.
- Установлена программа sudo. Пользователь, от имени которого выполняется установка, добавлен в группу sudo.

6.2. Установка локального сервера обновлений

Для установки локального сервера обновлений вам понадобится архив с установщиком PT Email Security.

Архив с установщиком входит в комплект поставки PT Email Security и имеет название в формате `ptsb.installer.<Версия ОС>.<Версия продукта>.tar.gz`, например `ptsb.installer.debian-12-amd64.5.30.0.177.tar.gz`.

Примечание. После установки вы можете узнать статус локального сервера обновлений с помощью команды `systemctl status pt-update-mirror.service` или просмотреть его журналы с помощью команды `journalctl -u pt-update-mirror.service`.

► Чтобы установить локальный сервер обновлений:

1. Скопируйте архив с установщиком PT Email Security в любой каталог на узле.
2. Перейдите в каталог с архивом, например:
`cd /home/user/ptsb-installer`
3. Распакуйте архив, например:
`tar pxvf ptsb.installer.debian-12-amd64.5.30.0.177.tar.gz`
4. Запустите установку локального сервера обновлений:
`sudo ./update-mirror/install.sh`

Установка сертификатов

Если для скачивания обновлений с локального сервера обновлений вы планируете использовать протокол HTTPS, необходимо:

1. Выпустить для локального сервера обновлений SSL-сертификат доверенного центра сертификации вашей организации.

Внимание! Если вы установили два локальных сервера обновлений, необходимо выпустить SSL-сертификат для каждого из них.

2. Если вы установили два локальных сервера обновлений и планируете настроить автоматический перенос обновлений между ними, добавить корневой сертификат доверенного центра сертификации вашей организации в список доверенных на узле локального сервера обновлений, расположенного в изолированном сегменте сети.
3. Добавить выпущенный SSL-сертификат для локального сервера обновлений.

SSL-сертификат должен соответствовать следующим требованиям:

- Сертификат и закрытый ключ должны быть представлены в формате PEM. Закрытый ключ должен быть незашифрованным и иметь длину не менее 2048 бит.
- Сертификат должен использовать алгоритм подписи SHA-256. Для шифрования ключей должен применяться алгоритм RSA.
- Включать область применения Digital Signature или Key Encipherment.
- Содержать в расширении Subject Alternative Name (SAN) следующие записи: IP-адрес узла локального сервера обновлений и его доменное имя (при наличии).
- Если используются промежуточные сертификаты, должна быть включена полная цепочка, от корневого до конечного сертификата.

- Чтобы добавить корневой сертификат доверенного центра сертификации в список доверенных на узле:

1. Скопируйте файл сертификата в каталог `/usr/local/share/ca-certificates/`.

2. Обновите список доверенных сертификатов:

```
sudo update-ca-certificates
```

- Чтобы добавить SSL-сертификат для локального сервера обновлений:

1. Измените названия файла сертификата и его ключа на `cert.crt` и `cert.key` соответственно.
2. Скопируйте файлы сертификата и его ключа в каталог `/etc/pt-update-mirror/https_certs/`.
3. Перезапустите локальный сервер обновлений:

```
sudo systemctl restart pt-update-mirror.service
```

6.3. Настройка локального сервера обновлений

После установки локального сервера обновлений вы можете настроить подключение к прокси-серверу, выбрать версии и компоненты PT Email Security для обновления или настроить время проверки обновлений.

Настройка подключения к прокси-серверу

► Чтобы настроить подключение к прокси-серверу:

1. Откройте файл `/etc/pt-update-mirror/config.json`.
2. В параметре `proxy` укажите адрес и порт прокси-сервера:
 - Если используется протокол HTTPS:


```
"proxy": "https://<IP-адрес прокси-сервера>:<Порт>"
```
 - Если для подключения используется протокол HTTP:


```
"proxy": "http://<IP-адрес прокси-сервера>:<Порт>"
```
3. Если требуется аутентификация на прокси-сервере, в параметрах `proxy-user` и `proxy-password` укажите учетные данные:


```
"proxy-user": "<Логин>",  
"proxy-password": "<Пароль>"
```
4. Сохраните изменения и закройте файл.
5. Перезапустите локальный сервер обновлений:


```
sudo systemctl restart pt-update-mirror.service
```

Если вы используете прокси-сервер с SSL-инспекцией, необходимо на узле локального сервера обновлений добавить корневой сертификат центра сертификации вашей организации в список доверенных.

► Чтобы добавить корневой сертификат центра сертификации в список доверенных на узле:

1. Скопируйте файл сертификата в каталог `/usr/local/share/ca-certificates/`.
2. Обновите список доверенных сертификатов:


```
sudo update-ca-certificates
```

Настройка скачивания обновлений PT Email Security

► Чтобы настроить скачивание PT Email Security:

1. Откройте файл `/etc/pt-update-mirror/config.json`.
2. Если необходимо скачивать обновления только для сертифицированных ФСТЭК версий PT Email Security, в секции `products` → `ptsb` укажите значения параметров (см. таблицу ниже):
 - В параметре `check_edition` укажите `true`.

- В параметре `edition` укажите `cert`.
- 3. Если необходимо скачивать обновления для определенных версий PT Email Security, в секции `products` → `ptsb` укажите значения параметров:
 - В параметре `count_number_on_version_parse` укажите количество старших разрядов в номере версии, которые определяют номер релиза.
 - В параметре `minimal_release` укажите номер самого раннего релиза, для которого необходимо скачивать обновления.
 - В параметре `store_release_versions` укажите количество версий, которое нужно скачивать и хранить на сервере для каждого релиза.
- 4. Если необходимо настроить скачивание обновлений для антивирусов, средств проверки Positive Technologies и образов VM, настройте значения параметров в соответствующих секциях:
 - Для обновлений антивирусных баз и баз знаний средств статического анализа объектов — в секции `products` → `ptms.db.*`.
 - Для обновлений баз знаний средств динамического анализа объектов — в секции `products` → `ptsb.db.*`.
 - Для обновлений образов VM — в секции `products` → `PTMS.sandbox.image.*`.
- 5. Сохраните изменения и закройте файл.
- 6. Перезапустите локальный сервер обновлений:


```
sudo systemctl restart pt-update-mirror.service
```

Изменение времени проверки обновлений

По умолчанию проверка обновлений выполняется каждые 15 минут.

Примечание. Вы можете проверить статус таймера обновлений с помощью команды `sudo systemctl status pt-update-mirror-update.timer`.

► Чтобы изменить время проверки обновлений:

1. Откройте файл `etc/systemd/system/pt-update-mirror-update.timer`.
2. В параметре `Timer` → `OnCalendar` укажите время получения обновлений в формате `systemd.timer`.
3. Сохраните изменения и закройте файл.
4. Примените изменения:


```
sudo systemctl daemon-reload
```
5. Перезапустите таймер обновлений:


```
sudo systemctl restart pt-update-mirror-update.timer
```


Конфигурационный файл config.json

Параметры локального сервера обновлений указаны в его конфигурационном файле `/etc/pt-update-mirror/config.json`.

Таблица 15. Параметры локального сервера обновлений

Параметр	Тип данных	Назначение
<code>db-path</code>	String	Каталог для сохранения обновлений. По умолчанию <code>/var/opt/pt/pt-update-mirror</code>
<code>http_disabled</code>	Boolean	Необходимо ли отключить обновление по протоколу HTTP при добавлении SSL-сертификата. По умолчанию <code>false</code>
<code>http_port</code>	Integer	Порт для запросов на обновление по протоколу HTTP. По умолчанию <code>8553</code>
<code>https_port</code>	Integer	Порт для запросов на обновление по протоколу HTTPS. По умолчанию <code>8743</code>
<code>log-level</code>	Enum	Уровень журналирования работы локального сервера обновлений: <code>DEBUG</code> , <code>INFO</code> (по умолчанию), <code>WARNING</code> , <code>ERROR</code>
<code>logrotate</code>	Enum	Способ ротации журнала: — <code>daily</code> — ежедневно в полночь; — <code>size</code> — при достижении файлом журнала размера 50 МБ. Примечание. Файл журнала расположен в каталоге <code>var/log/pt-update-mirror</code>
<code>proxy</code>	String	Адрес прокси-сервера
<code>proxy-mode</code>	Boolean	Включен ли режим перенаправления запросов. При включенном режиме локальный сервер обновлений пересылает полученные от PT Email Security запросы на сервер обновлений Positive Technologies (если запрос не добавлен в исключения в параметре <code>proxy-mode-blacklist</code>). По умолчанию <code>true</code>
<code>proxy-mode-blacklist</code>	List (String)	Путь к файлу со списком URL-запросов, которые не перенаправляются. По умолчанию <code>/telemetry/v1/push/</code>
<code>proxy-password</code>	String	Пароль для аутентификации на прокси-сервере
<code>proxy-user</code>	String	Логин для аутентификации на прокси-сервере

Параметр	Тип данных	Назначение
update-server	String	Адрес сервера обновлений Positive Technologies. По умолчанию <code>https://update.ptsecurity.com</code>
verify_ssl	Boolean	Проверять ли SSL-сертификат при подключении к серверу обновлений, указанному в параметре <code>update-server</code> . По умолчанию <code>true</code>
products → «Репозиторий»		
check_edition	Boolean	Необходимо ли учитывать редакцию версии, указанную в параметре <code>edition</code> . По умолчанию <code>true</code>
count_number_on_version_parse	Integer	Количество старших разрядов в номере версии, которые определяют номер релиза. При смене цифр в этих разрядах версия считается новым релизом. Например, при значении 2 для версии 5.9.0.67859 номером релиза будет 5.9. При значении 0 отдельные релизы не выделяются и количество скачиваемых и хранимых на сервере версий определяется параметром <code>store_release_versions</code>
edition	String	Редакция версии. По умолчанию скачиваются версии, для которых редакция не указана. Примечание. Если необходимо скачивать только версии с сертификатом ФСТЭК, вы можете указать значение <code>cert</code>
minimal_release	String	Номер самого раннего релиза, для которого скачиваются обновления. Например, при значении 5.9 будут скачиваться обновления для релизов 5.9, 5.10 и выше. Количество разрядов в номере релиза должно совпадать со значением, указанным в параметре <code>count_number_on_version_parse</code> . Примечание. Для отключения скачивания обновлений из репозитория вы можете указать заведомо высокий номер релиза, например <code>100.0</code>
order	Integer	Приоритет загрузки обновлений. Чем меньше значение, тем выше приоритет обновлений из этого репозитория
store_release_versions	Integer	Количество новых версий, которые скачиваются и хранятся на сервере для каждого релиза. При скачивании новой версии самая старая версия релиза удаляется с сервера. Например, если выпущены версии 5.9.0.13597, 5.9.1.63293, 5.9.2.68444, 5.10.0.4851, при значении 2 на сервере будут хра-

Параметр	Тип данных	Назначение
		наться для релиза 5.9 — версии 5.9.1.63293 и 5.9.2.68444, для релиза 5.10 — версия 5.10.0.4851. При значении 0 для каждого релиза будут скачиваться все версии. Примечание. Скачанные версии сохраняются в каталоге <Каталог обновлений>/products/<Репозиторий>/<Номер релиза>
synchronizer	Enum	Метод скачивания обновлений: — ComponentSynchronizer — для баз знаний средств проверки; — DockerSynchronizer; — PTMSDocsSynchronizer; — PTMSSynchronizer — для компонентов PT Email Security; — PackmanSynchronizer

Пример конфигурационного файла:

```
{
  "db-path": "/var/opt/pt/pt-update-mirror",
  "http_disabled": false,
  "http_port": 8553,
  "https_port": 8743,
  "log-level": "INFO",
  "logrotate": "daily",
  "proxy": "",
  "proxy-mode": true,
  "proxy-mode-blacklist": [
    "/telemetry/v1/push/"
  ],
  "proxy-password": "",
  "proxy-user": "",
  "update-server": "https://update.ptsecurity.com",
  "verify_ssl": true,
  "products": {
    "ptsb": {
      "check_edition": true,
      "count_number_on_version_parse": 2,
      "edition": "",
      "minimal_release": "5.8",
      "order": 1,
      "store_release_versions": 2,
      "synchronizer": "PTMSSynchronizer"
    },
    "ptms.db.*": {
      "count_number_on_version_parse": 2,
      "order": 1,
      "store_release_versions": 2,
      "synchronizer": "ComponentSynchronizer"
    },
    "ptsb.db.*": {
      "count_number_on_version_parse": 2,
      "order": 1,
      "store_release_versions": 2,
      "synchronizer": "ComponentSynchronizer"
    },
    "PTMS.sandbox.image.*": {
      "count_number_on_version_parse": 1,
      "order": 1,
      "store_release_versions": 1,
      "synchronizer": "ComponentSynchronizer"
    }
  }
}
```

}

6.4. Активация лицензии

Для скачивания обновлений с сервера Positive Technologies на локальном сервере обновлений должна быть активирована лицензия PT Email Security.

Примечание. Вы можете проверить статус активации лицензии, выполнив на локальном сервере обновлений команду `sudo /opt/pt/pt-update-mirror/bin/pt-update-mirror license view`.

Для активации лицензии PT Email Security вам понадобится серийный номер лицензии, который указывается в файле `serial number.txt` на установочном диске из комплекта поставки PT Email Security или высылается в электронном письме на адрес, указанный при заказе лицензии.

- ▶ Чтобы активировать лицензию PT Email Security на локальном сервере обновлений,

выполните команду:

- Если локальный сервер обновлений имеет прямой доступ к серверу обновлений Positive Technologies:

```
sudo /opt/pt/pt-update-mirror/bin/pt-update-mirror license activate --serial-number
'<Серийный номер лицензии>'
```

- Если используется прокси-сервер:

```
sudo /opt/pt/pt-update-mirror/bin/pt-update-mirror license activate --serial-number
'<Серийный номер лицензии>' --proxy <IP-адрес прокси-сервера>:<Порт> --proxy-user <Логин>
--proxy-password <Пароль>
```

Например:

```
sudo /opt/pt/pt-update-mirror/bin/pt-update-mirror license activate --serial-number
'xxxxxx-xxxxxx-xxxxxx-xxxxxx-xxxxxx-xxxxxx-xxxxxxxxxxxx' --proxy http://
192.0.2.15:8080 --proxy-user Ivanov --proxy-password P@ssw0rd
```

6.5. Перенос обновлений в изолированный сегмент сети

Если между локальными серверами обновлений есть сетевое взаимодействие, вы можете настроить автоматический перенос обновлений в изолированный сегмент сети. Если сетевая связность отсутствует, вы можете перенести обновления вручную при помощи внешнего носителя.

Настройка автоматического переноса обновлений

Если между локальными серверами есть сетевое взаимодействие, вы можете настроить подключение локального сервера обновлений, расположенного в изолированном сегменте сети, к серверу обновлений в DMZ. Это позволит автоматически передавать в закрытый сегмент сети обновления PT Email Security, скачанные с сервера обновлений Positive Technologies.

Внимание! Если в вашей информационной системе используется межсетевой экран или другие средства контроля сетевого трафика, требуется настроить в них правила, разрешающие передачу трафика от локального сервера обновлений в DMZ к серверу обновлений в изолированном сегменте сети. По умолчанию для протокола HTTPS используется порт TCP 8743, для протокола HTTP — порт TCP 8553.

Инструкцию необходимо выполнить на узле локального сервера обновлений в закрытом сегменте сети.

► Чтобы настроить подключение к локальному серверу обновлений в DMZ:

1. Откройте файл `/etc/pt-update-mirror/config.json`.
2. В параметре `update-server` укажите адрес локального сервера обновлений в DMZ:
 - Если используется протокол HTTPS:


```
"update-server": "https://<Адрес локального сервера обновлений>:<Порт>"
```
 - Если для подключения используется протокол HTTP:


```
"update-server": "http://<Адрес локального сервера обновлений>:<Порт>"
```
3. Если используется протокол HTTPS, с помощью параметра `verify_ssl` настройте проверку SSL-сертификата локального сервера обновлений в DMZ:
 - Если требуется проверять сертификат:


```
"verify_ssl": true
```
 - Если проверять сертификат не требуется:


```
"verify_ssl": false
```
4. Сохраните изменения и закройте файл.
5. Перезапустите локальный сервер обновлений:


```
sudo systemctl restart pt-update-mirror.service
```

Перенос обновлений вручную

Если между локальным сервером обновлений в DMZ и сервером обновлений в изолированном сегменте сети отсутствует сетевая связность, вам нужно вручную переносить обновления PT Email Security в закрытый сегмент. Для переноса обновлений необходимо:

1. На сервере обновлений, который имеет доступ к серверу обновлений Positive Technologies, запустить скачивание обновлений PT Email Security.

Внимание! Для скачивания обновлений с сервера Positive Technologies на локальном сервере обновлений должна быть активирована лицензия PT Email Security.

2. На том же сервере обновлений экспортировать загруженные обновления в файл.
3. Перенести при помощи внешнего носителя полученный файл с обновлениями на узел локального сервера обновлений в изолированном сегменте сети.
4. На сервере обновлений в изолированном сегменте сети импортировать обновления из файла.

- ▶ Чтобы запустить скачивание обновлений с сервера Positive Technologies,

выполните команду:

```
sudo /opt/pt/pt-update-mirror/bin/pt-update-mirror repository update
```

Примечание. Вы можете просмотреть информацию о скачанных обновлениях, выполнив команду `sudo /opt/pt/pt-update-mirror/bin/pt-update-mirror repository view-registry`.

- ▶ Чтобы экспортировать обновления в файл,

выполните команду:

- Если требуется экспортировать обновления и лицензию PT Email Security, а также обновления баз средств проверки:

```
sudo /opt/pt/pt-update-mirror/bin/pt-update-mirror repository export <Путь к архиву>
```

- Если требуется экспортировать только лицензию PT Email Security:

```
sudo /opt/pt/pt-update-mirror/bin/pt-update-mirror repository export --only-licenses <Путь к архиву>
```

- Если требуется экспортировать только обновления баз средств проверки:

```
sudo /opt/pt/pt-update-mirror/bin/pt-update-mirror repository export --only-data-bases <Путь к архиву>
```

Например:

```
sudo /opt/pt/pt-update-mirror/bin/pt-update-mirror repository export --only-data-bases /home/user/tmp/update.tar.gz
```

- ▶ Чтобы импортировать обновления из файла,

выполните команду:

- Если требуется импортировать лицензию PT Email Security:

```
sudo -- bash -c 'yes | /opt/pt/pt-update-mirror/bin/pt-update-mirror repository import --only-licenses <Путь к архиву>'
```

- Если из файла требуется импортировать все:

```
sudo -- bash -c 'yes | /opt/pt/pt-update-mirror/bin/pt-update-mirror repository import <Путь к архиву>'
```

Например:

```
sudo -- bash -c 'yes | /opt/pt/pt-update-mirror/bin/pt-update-mirror repository import /home/user/tmp/update.tar.gz'
```

6.6. Выбор локального сервера в качестве источника обновлений

Для выбора локального сервера в качестве источника обновлений необходимо:

1. На основном узле PT Email Security указать адрес локального сервера в качестве источника обновлений.

Примечание. Вы можете узнать адрес источника обновлений PT Email Security, выполнив на основном узле команду `sudo ptmsctl product settings view`. Адрес будет указан в параметре `update-server`.

2. Если для скачивания обновлений вы планируете использовать протокол HTTPS:
 - Добавить корневой сертификат доверенного центра сертификации организации (которым подписан SSL-сертификат локального сервера обновлений) в список доверенных на каждом узле PT Email Security.
 - Добавить этот же сертификат в PT Email Security.
3. Если для скачивания обновлений вы планируете использовать протокол HTTP, на каждом узле PT Email Security указать адрес локального сервера обновлений в параметрах среды `containerd`.

Добавление адреса локального сервера обновлений в PT Email Security

Инструкцию необходимо выполнить на основном узле PT Email Security.

- Чтобы в PT Email Security указать адрес локального сервера в качестве источника обновлений,

выполните команду:

- Если для скачивания обновлений используется протокол HTTP:


```
sudo ptmsctl product settings apply --update-server http://<IP-адрес или FQDN>:8553
```
- Если используется протокол HTTPS:


```
sudo ptmsctl product settings apply --update-server https://<IP-адрес или FQDN>:8743
```

Появятся сообщения о применении параметров.

Добавление корневого сертификата в список доверенных

Инструкцию необходимо выполнить на основном, резервных и всех дополнительных узлах PT Email Security.

- Чтобы добавить корневой сертификат доверенного центра сертификации в список доверенных на узле:
 1. Скопируйте файл сертификата в каталог `/usr/local/share/ca-certificates/`.
 2. Обновите список доверенных сертификатов:


```
sudo update-ca-certificates
```

Добавление корневого сертификата в PT Email Security

Инструкцию необходимо выполнить на основном узле PT Email Security.

- ▶ Чтобы добавить корневой сертификат доверенного центра сертификации вашей организации в PT Email Security,

выполните команду:

```
sudo ptmsctl product settings apply --proxy-ca-crt '<Полный путь к файлу корневого сертификата>'
```

Добавление адреса локального сервера обновлений в параметры среды containerd

Инструкцию необходимо выполнить на основном, резервных и всех дополнительных узлах PT Email Security.

- ▶ Чтобы указать адрес локального сервера обновлений в параметрах среды containerd:

1. Создайте на узле файл `/etc/containerd/certs.d/<IP-адрес или FQDN>:8553/hosts.toml`.

2. Добавьте в файл строки:

```
server = "http://<IP-адрес или FQDN>:8553"
[host."http://<IP-адрес или FQDN>:8553"]
  capabilities = ["pull", "resolve"]
```

3. Сохраните изменения и закройте файл.

4. Перезапустите службу containerd:

```
sudo systemctl restart containerd
```

Примечание. Вы можете узнать состояние службы, выполнив команду `sudo service containerd status`.

7. Развертывание PT Email Security с помощью установщика

В разделе приведены инструкции по развертыванию различных конфигураций PT Email Security с помощью установщика.

При развертывании вам необходимо придерживаться следующей последовательности действий:

1. Если для обновления PT Email Security требуется использовать локальный сервер обновлений, установить его, настроить и указать лицензию PT Email Security.

Внимание! Поддерживается локальный сервер обновлений версии 2.0 и выше (входит в комплект поставки PT Email Security).

2. Установить выбранную конфигурацию PT Email Security.

В процессе установки потребуется доступ к серверам обслуживания Positive Technologies (напрямую, через прокси-сервер или локальный сервер обновлений). Также в процессе установки вам потребуется:

- Если для доступа к внешним ресурсам требуется использовать прокси-сервер, указать параметры подключения к прокси-серверу.

Этот же прокси-сервер будет использоваться при подключении к серверам обслуживания Positive Technologies или локальному серверу обновлений.

- Если для обновления PT Email Security требуется использовать локальный сервер обновлений, указать его адрес.
- Активировать лицензию PT Email Security.

3. Если для входа пользователей в PT Email Security требуется использовать внешний PT MC, подключить его.

В этом разделе

[Подготовка к развертыванию \(см. раздел 7.1\)](#)

[Базовая конфигурация \(см. раздел 7.2\)](#)

[Высоконагруженная конфигурация \(см. раздел 7.3\)](#)

[Отказоустойчивый кластер для высоконагруженной конфигурации \(см. раздел 7.4\)](#)

[Дополнительные действия при развертывании \(см. раздел 7.5\)](#)

7.1. Подготовка к развертыванию

Перед развертыванием вам необходимо подготовить каждый узел выбранной конфигурации, на который будут устанавливаться компоненты PT Email Security:

1. Установить на узле одну из ОС, рекомендованных в программных требованиях PT Email Security.
2. Скопировать на каждый узел архив с установщиком и распаковать его.
3. Если в вашей информационной системе для доступа в интернет используется прокси-сервер, настроить подключение менеджера обновлений ОС к этому прокси-серверу.
4. Проверить доступ с узла к серверам обслуживания Positive Technologies.

В этом разделе

[Проверка доступа к серверам обслуживания \(см. раздел 7.1.1\)](#)

[Распаковка архива с установщиком \(см. раздел 7.1.2\)](#)

[Настройка подключения менеджера обновлений ОС к прокси-серверу \(см. раздел 7.1.3\)](#)

7.1.1. Проверка доступа к серверам обслуживания

В процессе установки, обновления и проверки лицензии PT Email Security обращается к серверам обслуживания Positive Technologies на поддоменах сайта ptsecurity.com.

Внимание! Если в вашей информационной системе используется межсетевой экран или другие средства контроля сетевого трафика, необходимо настроить в них правила, разрешающие доступ по протоколу HTTPS к серверам Positive Technologies со всех узлов PT Email Security.

► Чтобы проверить доступ к серверам обслуживания PT Email Security:

1. Проверьте подключение к поддомену update:

```
wget -Sq -O /dev/null https://update.ptsecurity.com/test
```
2. Если код ответа отличается от 200 OK, настройте доступ и проверьте подключение повторно.

7.1.2. Распаковка архива с установщиком

Архив с установщиком входит в комплект поставки PT Email Security и имеет название в формате `ptsb.installer.<Версия ОС>.<Версия продукта>.tar.gz`, например `ptsb.installer.debian-12-amd64.5.30.0.177.tar.gz`.

► Чтобы распаковать архив с установщиком PT Email Security:

1. Скопируйте архив с установщиком в любой каталог на узле.

2. Перейдите в каталог с архивом, например:

```
cd /home/user/ptsb-installer
```

3. Распакуйте архив, например:

```
tar pxvf ptsb.installer.debian-12-amd64.5.30.0.177.tar.gz
```

7.1.3. Настройка подключения менеджера обновлений ОС к прокси-серверу

Если в вашей информационной системе подключение к интернету выполняется через прокси-сервер, вам нужно настроить подключение менеджера обновлений ОС к прокси-серверу.

► Чтобы настроить подключение менеджера обновлений ОС к прокси-серверу:

1. Перейдите в каталог с установщиком PT Email Security, например:

```
cd /home/user/ptsb-installer
```

2. Запустите скрипт для настройки, указав параметры подключения к прокси-серверу:

```
sudo ./setup-apt-proxy.sh --proxy-addr <Адрес прокси-сервера>:<Порт> --proxy-user <Логин для подключения к прокси-серверу> --proxy-pass <Пароль для подключения к прокси-серверу>
```

Например:

```
sudo ./setup-apt-proxy.sh --proxy-addr http://192.0.2.108:3128 --proxy-user ivanov --proxy-pass P@ssw0rd
```

Подключение менеджера обновлений ОС к прокси-серверу настроено.

7.2. Базовая конфигурация

Базовая конфигурация PT Email Security (All-in-One) состоит из одного основного узла с функцией поведенческого анализа. Для развертывания базовой конфигурации вам необходимо:

1. Подготовить основной узел к установке.
2. Установить на основной узел гипервизор Xen.
3. Установить на основной узел компоненты PT Email Security.
4. Активировать на основном узле функцию поведенческого анализа.

В этом разделе

[Установка гипервизора Xen на основной узел \(см. раздел 7.2.1\)](#)

[Установка компонентов PT Email Security на основной узел \(см. раздел 7.2.2\)](#)

7.2.1. Установка гипервизора Xen на основной узел

Для выполнения поведенческого анализа на узле необходимо установить гипервизор Xen. Требования к аппаратным ресурсам узла зависят от количества одновременно запускаемых в гипервизоре виртуальных машин. На основном узле одновременно может запускаться не более 15 виртуальных машин.

Определение требований к аппаратным ресурсам

► Чтобы определить требования к аппаратным ресурсам узла:

1. Перейдите в каталог с установщиком PT Email Security, например:
`cd /home/user/ptsb-installer`
2. Запустите скрипт для определения требований к аппаратным ресурсам узла:
 - Если необходимо определить, сколько виртуальных машин могут одновременно работать на узле исходя из его аппаратных ресурсов:
`sudo xen/check-system-requirements.sh --get-max-vm`
 - Если необходимо определить, сколько аппаратных ресурсов требуется для одновременной работы определенного количества виртуальных машин:
`sudo xen/check-system-requirements.sh --vm-count <Количество виртуальных машин>`

Примечание. Подробная справка доступна по команде `sudo xen/check-system-requirements.sh -h`.

Установка гипервизора Xen

► Чтобы установить гипервизор Xen:

1. Перейдите в каталог с установщиком PT Email Security, например:
`cd /home/user/ptsb-installer`
2. Запустите скрипт для проверки соответствия узла аппаратным требованиям:
`sudo xen/check-system-requirements.sh`
3. Если узел соответствует аппаратным требованиям, запустите скрипт установки гипервизора:
`sudo xen/install.sh --vm-count <Количество виртуальных машин>`

Примечание. Подробная справка доступна по команде `sudo xen/install.sh -h`.

4. По завершении работы скрипта нажмите клавишу Enter.
Узел будет перезагружен.
5. Если требуется, введите логин и пароль загрузчика.
Гипервизор Xen установлен.

7.2.2. Установка компонентов PT Email Security на основной узел

Внимание! Имя узла в операционной системе (hostname) должно отличаться от имен других узлов PT Email Security в рамках одной конфигурации. Изменение имени узла после установки компонентов PT Email Security приведет к неработоспособности компонентов PT Email Security на этом узле.

Для выполнения инструкции вам понадобится серийный номер лицензии PT Email Security, приобретенной вашей организацией. Серийный номер высылается на адрес электронной почты, указанный при заказе лицензии, или указывается в файле `serial number.txt` на установочном диске из комплекта поставки.

► Чтобы установить компоненты PT Email Security на основной узел:

1. Перейдите в каталог с установщиком PT Email Security, например:
`cd /home/user/ptsb-installer`
2. Запустите мастер установки PT Email Security:
`sudo ./wizard`
3. Выберите язык мастера установки и нажмите клавишу Enter.
4. Выберите метод скачивания обновлений PT Email Security с сайта Positive Technologies и нажмите клавишу Enter.

Примечание. Вы можете выбрать скачивание напрямую с сайта Positive Technologies, через прокси-сервер или через локальный сервер обновлений.

5. Если вы выбрали вариант скачивания через прокси-сервер:
 - Введите IP-адрес прокси-сервера и нажмите клавишу Enter.
 - Последовательно введите логин и пароль учетной записи для доступа к серверу, подтверждая ввод клавишей Enter.
 - Если вы используете прокси-сервер с SSL-инспекцией, укажите полный путь к пользовательскому корневому сертификату формата PEM и нажмите клавишу Enter.
6. Если вы выбрали вариант скачивания через локальный сервер обновлений, введите его IP-адрес и нажмите клавишу Enter.
7. Введите серийный номер лицензии (без кавычек) и нажмите клавишу Enter.
8. Если вы планируете настраивать отказоустойчивый кластер, укажите его виртуальный адрес и нажмите клавишу Enter.
9. Введите `y` и нажмите клавишу Enter.

Начнется установка PT Email Security. По завершении появится сообщение об успешной установке.

Компоненты PT Email Security установлены на основной узел.

7.3. Высоконагруженная конфигурация

Высоконагруженная конфигурация PT Email Security состоит из основного узла (без функции поведенческого анализа) и одного или нескольких дополнительных узлов для поведенческого анализа файлов. Для развертывания высоконагруженной конфигурации PT Email Security вам необходимо:

1. Развернуть основной узел (без функции поведенческого анализа):
 - Подготовить основной узел к установке.
 - Установить на основной узел компоненты PT Email Security.
2. Развернуть дополнительные узлы:
 - Подготовить каждый дополнительный узел к установке.
 - Установить на каждый дополнительный узел гипервизор Xen.
 - Установить на каждый дополнительный узел компоненты PT Email Security.
3. Активировать на дополнительных узлах функцию поведенческого анализа.

В этом разделе

[Установка компонентов PT Email Security на основной узел \(см. раздел 7.3.1\)](#)

[Установка гипервизора Xen на дополнительный узел \(см. раздел 7.3.2\)](#)

[Установка компонентов PT Email Security на дополнительный узел \(см. раздел 7.3.3\)](#)

7.3.1. Установка компонентов PT Email Security на основной узел

Внимание! Имя узла в операционной системе (hostname) должно отличаться от имен других узлов PT Email Security в рамках одной конфигурации. Изменение имени узла после установки компонентов PT Email Security приведет к неработоспособности компонентов PT Email Security на этом узле.

Для выполнения инструкции вам понадобится серийный номер лицензии PT Email Security, приобретенной вашей организацией. Серийный номер высылается на адрес электронной почты, указанный при заказе лицензии, или указывается в файле `serial number.txt` на установочном диске из комплекта поставки.

► Чтобы установить компоненты PT Email Security на основной узел:

1. Перейдите в каталог с установщиком PT Email Security, например:
`cd /home/user/ptsb-installer`
2. Запустите мастер установки PT Email Security:
`sudo ./wizard`

3. Выберите язык мастера установки и нажмите клавишу Enter.
4. Выберите метод скачивания обновлений PT Email Security с сайта Positive Technologies и нажмите клавишу Enter.

Примечание. Вы можете выбрать скачивание напрямую с сайта Positive Technologies, через прокси-сервер или через локальный сервер обновлений.

5. Если вы выбрали вариант скачивания через прокси-сервер:
 - Введите IP-адрес прокси-сервера и нажмите клавишу Enter.
 - Последовательно введите логин и пароль учетной записи для доступа к серверу, подтверждая ввод клавишей Enter.
 - Если вы используете прокси-сервер с SSL-инспекцией, укажите полный путь к пользовательскому корневому сертификату формата PEM и нажмите клавишу Enter.
6. Если вы выбрали вариант скачивания через локальный сервер обновлений, введите его IP-адрес и нажмите клавишу Enter.
7. Введите серийный номер лицензии (без кавычек) и нажмите клавишу Enter.
8. Если вы планируете настраивать отказоустойчивый кластер, укажите его виртуальный адрес и нажмите клавишу Enter.
9. Введите `y` и нажмите клавишу Enter.

Начнется установка PT Email Security. По завершении появится сообщение об успешной установке.

Компоненты PT Email Security установлены на основной узел.

7.3.2. Установка гипервизора Xen на дополнительный узел

Для выполнения поведенческого анализа на узле необходимо установить гипервизор Xen.

Примечание. По умолчанию на одном дополнительном узле одновременно может запускаться не более 15 виртуальных машин. Вы можете увеличить это количество до 45 при настройке поведенческого анализа после завершения развертывания всех узлов в конфигурации.

Определение требований к аппаратным ресурсам

Требования к аппаратным ресурсам узла зависят от количества одновременно запускаемых в гипервизоре виртуальных машин.

► Чтобы определить требования к аппаратным ресурсам узла:

1. Перейдите в каталог с установщиком PT Email Security, например:
`cd /home/user/ptsb-installer`
2. Запустите скрипт для определения требований к аппаратным ресурсам узла:

- Если необходимо определить, сколько виртуальных машин могут одновременно работать на узле исходя из его аппаратных ресурсов:
`sudo xen/check-system-requirements.sh --slave --get-max-vm`
- Если необходимо определить, сколько аппаратных ресурсов требуется для одновременной работы определенного количества виртуальных машин:
`sudo xen/check-system-requirements.sh --slave --vm-count <Количество виртуальных машин>`

Примечание. Подробная справка доступна по команде `sudo xen/check-system-requirements.sh -h`.

Установка гипервизора Xen

► Чтобы установить гипервизор Xen:

1. Перейдите в каталог с установщиком PT Email Security, например:
`cd /home/user/ptsb-installer`
2. Запустите скрипт для проверки соответствия узла аппаратным требованиям:
`sudo xen/check-system-requirements.sh --slave`
3. Если узел соответствует аппаратным требованиям, запустите скрипт установки гипервизора:
`sudo xen/install.sh --slave --vm-count <Количество виртуальных машин>`

Примечание. Подробная справка доступна по команде `sudo xen/install.sh -h`.

4. По завершении работы скрипта нажмите клавишу Enter.

Узел будет перезагружен.

5. Если требуется, введите логин и пароль загрузчика.

Гипервизор Xen установлен.

7.3.3. Установка компонентов PT Email Security на дополнительный узел

Внимание! Имя узла в операционной системе (hostname) должно отличаться от имен других узлов PT Email Security в рамках одной конфигурации. Изменение имени узла после установки компонентов PT Email Security приведет к неработоспособности компонентов PT Email Security на этом узле.

Установка компонентов PT Email Security на дополнительный узел выполняется при помощи специальной команды. Эту команду нужно сгенерировать на основном узле и затем запустить на дополнительном.

Генерация команды для установки компонентов PT Email Security

Инструкцию необходимо выполнять на основном узле.

Внимание! Команда действует два часа. Повторная генерация команды делает недействительной ранее сгенерированную команду.

► Чтобы получить команду для установки компонентов PT Email Security:

1. Перейдите в каталог с установщиком PT Email Security, например:

```
cd /home/user/ptsb-installer
```

2. Запустите скрипт для генерации команды:

```
sudo ./k8s-gen-token.sh
```

Пример сгенерированной команды:

```
./k8s-join-node.sh --cluster-ip 192.0.2.55 --token ijqr4l.vizd2...1vi66
```

Запуск команды для установки компонентов PT Email Security

Инструкцию необходимо выполнять на дополнительном узле от имени суперпользователя (root).

► Чтобы установить компоненты PT Email Security:

1. Перейдите в каталог с установщиком PT Email Security, например:

```
cd /home/user/ptsb-installer
```

2. Выполните полученную ранее команду, например:

```
sudo ./k8s-join-node.sh --cluster-ip 192.0.2.55 --token ijqr4l.vizd2...1vi66
```

Примечание. Если для доступа к внешним ресурсам в сети организации используется прокси-сервер, в команду для установки дополнительных узлов необходимо добавить параметры `--proxy-addr 'http://<IP-адрес прокси-сервера>:<Порт>' --proxy-user '<Логин>' --proxy-password '<Пароль>'`.

Компоненты PT Email Security установлены.

7.4. Отказоустойчивый кластер для высоконагруженной конфигурации

Отказоустойчивый кластер для высоконагруженной конфигурации PT Email Security состоит из основного узла (без функции поведенческого анализа), двух резервных узлов и одного или нескольких дополнительных узлов для поведенческого анализа файлов. Для развертывания отказоустойчивого кластера для высоконагруженной конфигурации PT Email Security вам необходимо:

1. Развернуть основной узел (без функции поведенческого анализа):
 - Подготовить основной узел к установке.
 - Установить на основной узел службу Keepalived.
 - Установить на основной узел компоненты PT Email Security.
2. Развернуть два резервных узла:
 - Подготовить оба резервных узла к установке.
 - Установить на оба резервных узла службу Keepalived.
 - Установить на оба резервных узла компоненты PT Email Security.
3. Развернуть дополнительные узлы:
 - Подготовить каждый дополнительный узел к установке.
 - Установить на каждый дополнительный узел гипервизор Xen.
 - Установить на каждый дополнительный узел компоненты PT Email Security.
4. Активировать на дополнительных узлах функцию поведенческого анализа.

В этом разделе

[Установка службы Keepalived на основной или резервный узел \(см. раздел 7.4.1\)](#)

[Установка компонентов PT Email Security на основной узел \(см. раздел 7.4.2\)](#)

[Установка компонентов PT Email Security на резервный узел \(см. раздел 7.4.3\)](#)

[Установка гипервизора Xen на дополнительный узел \(см. раздел 7.4.4\)](#)

[Установка компонентов PT Email Security на дополнительный узел \(см. раздел 7.4.5\)](#)

7.4.1. Установка службы Keepalived на основной или резервный узел

Служба Keepalived обеспечивает работоспособность PT Email Security в случае сбоев его отдельных компонентов или узлов.

Внимание! IP-адреса основного и резервных узлов должны находиться в адресном пространстве одной и той же сети или подсети.

Перед выполнением инструкции вам нужно выделить в сетевой инфраструктуре организации виртуальный IP-адрес для PT Email Security. По этому IP-адресу, в частности, будет доступен веб-интерфейс продукта.

Внимание! Виртуальный IP-адрес должен отличаться от IP-адресов других узлов PT Email Security.

► Чтобы установить службу Keepalived на основной (резервный) узел:

1. Перейдите в каталог с установщиком PT Email Security, например:

```
cd /home/user/ptsb-installer
```

2. Запустите скрипт `install-keepalived.sh` для установки службы:

```
sudo ./install-keepalived.sh --virtual-ip <Виртуальный IP-адрес> --interface <Название  
сетевого интерфейса этого IP-адреса>
```

Например:

```
sudo ./install-keepalived.sh --virtual-ip 192.0.2.55 --interface eth0
```

По завершении работы скрипта появится сообщение об успешной установке службы.

Служба Keepalived установлена на основной (резервный) узел.

7.4.2. Установка компонентов PT Email Security на основной узел

Внимание! Имя узла в операционной системе (hostname) должно отличаться от имен других узлов PT Email Security в рамках одной конфигурации. Изменение имени узла после установки компонентов PT Email Security приведет к неработоспособности компонентов PT Email Security на этом узле.

Для выполнения инструкции вам понадобится серийный номер лицензии PT Email Security, приобретенной вашей организацией. Серийный номер высылается на адрес электронной почты, указанный при заказе лицензии, или указывается в файле `serial number.txt` на установочном диске из комплекта поставки.

► Чтобы установить компоненты PT Email Security на основной узел:

1. Перейдите в каталог с установщиком PT Email Security, например:

```
cd /home/user/ptsb-installer
```

2. Запустите мастер установки PT Email Security:

```
sudo ./wizard
```

3. Выберите язык мастера установки и нажмите клавишу Enter.

4. Выберите метод скачивания обновлений PT Email Security с сайта Positive Technologies и нажмите клавишу Enter.

Примечание. Вы можете выбрать скачивание напрямую с сайта Positive Technologies, через прокси-сервер или через локальный сервер обновлений.

5. Если вы выбрали вариант скачивания через прокси-сервер:
 - Введите IP-адрес прокси-сервера и нажмите клавишу Enter.
 - Последовательно введите логин и пароль учетной записи для доступа к серверу, подтверждая ввод клавишей Enter.
 - Если вы используете прокси-сервер с SSL-инспекцией, укажите полный путь к пользовательскому корневому сертификату формата PEM и нажмите клавишу Enter.
6. Если вы выбрали вариант скачивания через локальный сервер обновлений, введите его IP-адрес и нажмите клавишу Enter.
7. Введите серийный номер лицензии (без кавычек) и нажмите клавишу Enter.
8. Если вы планируете настраивать отказоустойчивый кластер, укажите его виртуальный адрес и нажмите клавишу Enter.
9. Введите `y` и нажмите клавишу Enter.

Начнется установка PT Email Security. По завершении появится сообщение об успешной установке.

Компоненты PT Email Security установлены на основной узел.

7.4.3. Установка компонентов PT Email Security на резервный узел

Внимание! Имя узла в операционной системе (hostname) должно отличаться от имен других узлов PT Email Security в рамках одной конфигурации. Изменение имени узла после установки компонентов PT Email Security приведет к неработоспособности компонентов PT Email Security на этом узле.

Установка компонентов PT Email Security на резервный узел выполняется при помощи специальной команды. Эту команду нужно сгенерировать на основном узле и затем запустить на резервном.

Генерация команды для установки компонентов PT Email Security

Внимание! Команда действует два часа. Повторная генерация команды делает недействительной ранее сгенерированную команду.

Инструкцию необходимо выполнять на основном узле.

- ▶ Чтобы получить команду для установки компонентов PT Email Security на резервный узел:

1. Перейдите в каталог с установщиком PT Email Security, например:

```
cd /home/user/ptsb-installer
```

2. Запустите скрипт `k8s-gen-token.sh` для генерации команды:

```
sudo ./k8s-gen-token.sh --with-master-role
```

Пример сгенерированной команды:

```
./k8s-join-node.sh --cluster-ip 192.0.2.15 --token ijqr3l.viz...i66 --with-master-role --certificate-key 7f3e58...14e2b3f
```

Запуск команды для установки компонентов PT Email Security

Инструкцию необходимо выполнять на резервном узле от имени суперпользователя (root).

- ▶ Чтобы установить компоненты PT Email Security на резервный узел:

1. Перейдите в каталог с установщиком PT Email Security, например:

```
cd /home/user/ptsb-installer
```

2. Выполните полученную ранее команду, например:

```
./k8s-join-node.sh --cluster-ip 192.0.2.15 --token ijqr3l.viz...i66 --with-master-role --certificate-key 7f3e58...14e2b3f
```

Примечание. Если для доступа к внешним ресурсам в сети организации используется прокси-сервер, в команду для установки дополнительных узлов необходимо добавить параметры `--proxy-addr 'http://<IP-адрес прокси-сервера>:<Порт>' --proxy-user '<Логин>' --proxy-password '<Пароль>'`.

Компоненты PT Email Security установлены на резервный узел.

7.4.4. Установка гипервизора Xen на дополнительный узел

Для выполнения поведенческого анализа на узле необходимо установить гипервизор Xen.

Примечание. По умолчанию на одном дополнительном узле одновременно может запускаться не более 15 виртуальных машин. Вы можете увеличить это количество до 45 при настройке поведенческого анализа после завершения развертывания всех узлов в конфигурации.

Определение требований к аппаратным ресурсам

Требования к аппаратным ресурсам узла зависят от количества одновременно запускаемых в гипервизоре виртуальных машин.

► Чтобы определить требования к аппаратным ресурсам узла:

1. Перейдите в каталог с установщиком PT Email Security, например:

```
cd /home/user/ptsb-installer
```

2. Запустите скрипт для определения требований к аппаратным ресурсам узла:

- Если необходимо определить, сколько виртуальных машин могут одновременно работать на узле исходя из его аппаратных ресурсов:

```
sudo xen/check-system-requirements.sh --slave --get-max-vm
```

- Если необходимо определить, сколько аппаратных ресурсов требуется для одновременной работы определенного количества виртуальных машин:

```
sudo xen/check-system-requirements.sh --slave --vm-count <Количество виртуальных машин>
```

Примечание. Подробная справка доступна по команде `sudo xen/check-system-requirements.sh -h`.

Установка гипервизора Xen

► Чтобы установить гипервизор Xen:

1. Перейдите в каталог с установщиком PT Email Security, например:

```
cd /home/user/ptsb-installer
```

2. Запустите скрипт для проверки соответствия узла аппаратным требованиям:

```
sudo xen/check-system-requirements.sh --slave
```

3. Если узел соответствует аппаратным требованиям, запустите скрипт установки гипервизора:

```
sudo xen/install.sh --slave --vm-count <Количество виртуальных машин>
```

Примечание. Подробная справка доступна по команде `sudo xen/install.sh -h`.

4. По завершении работы скрипта нажмите клавишу Enter.

Узел будет перезагружен.

5. Если требуется, введите логин и пароль загрузчика.

Гипервизор Xen установлен.

7.4.5. Установка компонентов PT Email Security на дополнительный узел

Внимание! Имя узла в операционной системе (hostname) должно отличаться от имен других узлов PT Email Security в рамках одной конфигурации. Изменение имени узла после установки компонентов PT Email Security приведет к неработоспособности компонентов PT Email Security на этом узле.

Установка компонентов PT Email Security на дополнительный узел выполняется при помощи специальной команды. Эту команду нужно сгенерировать на основном узле и затем запустить на дополнительном.

Генерация команды для установки компонентов PT Email Security

Инструкцию необходимо выполнять на основном узле.

Внимание! Команда действует два часа. Повторная генерация команды делает недействительной ранее сгенерированную команду.

► Чтобы получить команду для установки компонентов PT Email Security:

1. Перейдите в каталог с установщиком PT Email Security, например:

```
cd /home/user/ptsb-installer
```

2. Запустите скрипт для генерации команды:

```
sudo ./k8s-gen-token.sh
```

Пример сгенерированной команды:

```
./k8s-join-node.sh --cluster-ip 192.0.2.55 --token ijqr4l.vizd2...1vi66
```

Запуск команды для установки компонентов PT Email Security

Инструкцию необходимо выполнять на дополнительном узле от имени суперпользователя (root).

► Чтобы установить компоненты PT Email Security:

1. Перейдите в каталог с установщиком PT Email Security, например:

```
cd /home/user/ptsb-installer
```

2. Выполните полученную ранее команду, например:

```
sudo ./k8s-join-node.sh --cluster-ip 192.0.2.55 --token ijqr4l.vizd2...1vi66
```

Примечание. Если для доступа к внешним ресурсам в сети организации используется прокси-сервер, в команду для установки дополнительных узлов необходимо добавить параметры `--proxy-addr 'http://<IP-адрес прокси-сервера>:<Порт>' --proxy-user '<Логин>' --proxy-password '<Пароль>'`.

Компоненты PT Email Security установлены.

7.5. Дополнительные действия при развертывании

После развертывания узлов выбранной конфигурации PT Email Security необходимо настроить поведенческий анализ объектов:

1. Активировать на узлах функцию поведенческого анализа.
2. Запустить скачивание и установку образов ВМ на узлах.

3. Если требуется, настроить максимальное количество ВМ, запускаемых на узлах.
4. Если требуется, настроить для ВМ объем памяти, выделяемой гостевой ОС.

Активация функции поведенческого анализа

На узлах, предназначенных для поведенческого анализа файлов, необходимо активировать функцию поведенческого анализа. Инструкции необходимо выполнять на основном узле.

- ▶ Чтобы получить список узлов, на которых установлены компоненты PT Email Security,

выполните команду:

```
sudo ptmsctl sandbox nodes list
```

Появится список узлов со статусом функции поведенческого анализа:

- `Behavioral analysis is enabled` — узел уже используется для поведенческого анализа;
- `Behavioral analysis is disabled` — узел не используется для поведенческого анализа;
- `Not ready for behavioral analysis to be enabled` — узел не может быть использован для поведенческого анализа (не установлен гипервизор Xen).

Последовательно активируйте функцию поведенческого анализа на узлах, предназначенных для поведенческого анализа файлов.

- ▶ Чтобы активировать функцию поведенческого анализа на узле,

выполните команду:

```
sudo ptmsctl sandbox nodes acquire <Имя узла>
```

Например:

```
sudo ptmsctl sandbox nodes acquire hostname
```

Если вы по ошибке активировали функцию поведенческого анализа на узле или необходимо изменить назначение узла, вы можете отключить эту функцию.

- ▶ Чтобы отключить функцию поведенческого анализа на узле,

выполните команду:

```
sudo ptmsctl sandbox nodes release <Имя узла>
```

Например:

```
sudo ptmsctl sandbox nodes release hostname
```

Скачивание и установка образов ВМ

Для поведенческого анализа файлов необходимо скачать образы ВМ с сервера обслуживания Positive Technologies и установить их на всех узлах с функцией поведенческого анализа. Инструкцию необходимо выполнять на основном узле.

- ▶ Чтобы запустить скачивание и установку образов ВМ на всех узлах с функцией поведенческого анализа,

выполните команду:

```
sudo ptmsctl sandbox force-generate-images
```

Скачивание и установка образов ВМ может занять продолжительное время. Процесс установки вы можете отслеживать через веб-интерфейс PT Email Security.

Настройка максимального количества ВМ, создаваемых на узлах

Для узлов PT Email Security с функцией поведенческого анализа вы можете указать максимальное количество ВМ, создаваемых одновременно на каждом узле. Предусмотрены инструкции для настройки максимального количества ВМ для основного узла, для всех дополнительных узлов и для каждого узла по отдельности. Все инструкции необходимо выполнять на основном узле.

На основном узле с функцией поведенческого анализа по умолчанию может создаваться не более 15 виртуальных машин одновременно. При необходимости вы можете уменьшить это количество.

Примечание. Если у вас настроена нестандартная конфигурация и часть функций основного узла вынесена на отдельный сервер, для изменения максимального количества ВМ, создаваемых на таком основном узле, необходимо использовать команду `sudo ptmsctl system components set -c traps-resource-plugin -p max_combo_traps=<Количество ВМ>`.

- ▶ Чтобы установить максимальное количество создаваемых ВМ для основного узла с функцией поведенческого анализа,

выполните команду:

```
sudo ptmsctl system components set -c traps-resource-plugin -p max_aio_traps=<Количество ВМ>
```

Например:

```
sudo ptmsctl system components set -c traps-resource-plugin -p max_aio_traps=2
```

На дополнительном узле для поведенческого анализа файлов по умолчанию может создаваться не более 15 виртуальных машин одновременно. При необходимости вы можете изменять это значение в диапазоне от 1 до 45.

Внимание! Если для поведенческого анализа файлов на узле используется образ с защищенной операционной системой Astra Linux Special Edition, максимальное количество одновременно создаваемых виртуальных машин на узле не должно превышать 30.

- ▶ Чтобы установить максимальное количество создаваемых ВМ для всех дополнительных узлов,

выполните команду:

```
sudo ptmsctl system components set -c traps-resource-plugin -p max_ba_traps=<Количество ВМ>
```

Например:

```
sudo ptmsctl system components set -c traps-resource-plugin -p max_ba_traps=45
```

Вы можете указать максимальное количество одновременно создаваемых ВМ отдельно для каждого узла в зависимости от его аппаратных ресурсов. Такой способ задания имеет самый высокий приоритет.

- ▶ Чтобы установить максимальное количество создаваемых ВМ отдельно для каждого узла с функцией поведенческого анализа,

выполните команду:

```
sudo ptmsctl system components set -c traps-resource-plugin -p max_node_traps='{\"Имя узла 1\": <Количество 1>, \"Имя узла 2\": <Количество 2>, ...}'
```

Например:

```
sudo ptmsctl system components set -c traps-resource-plugin -p max_node_traps='{\"main_host\": 5, \"ba_host_1\": 30, \"ba_host_2\": 45}'
```

Настройка объема памяти гостевой ОС

Для запуска одной виртуальной машины по умолчанию требуется 6 ГБ памяти ОЗУ, из них 2 ГБ используют службы поведенческого анализа и еще 4 ГБ выделяется гостевой операционной системе виртуальной машины. При необходимости вы можете изменить объем памяти гостевой операционной системы на всех узлах с функцией поведенческого анализа. Инструкцию необходимо выполнять на основном узле.

- ▶ Чтобы изменить объем памяти, выделяемой гостевой ОС, на всех узлах с функцией поведенческого анализа,

выполните команду:

```
sudo ptmsctl system components set -c sandbox-creator -p vm_memory_max_mb=<Объем памяти в МБ>
```

Например:

```
sudo ptmsctl system components set -c sandbox-creator -p vm_memory_max_mb=2048
```

После изменить объема памяти, выделяемой гостевой ОС, начнется перестроение и установка образов ВМ, что может занять продолжительное время. Процесс установки вы можете отслеживать через веб-интерфейс PT Email Security.

8. Первоначальная настройка PT Email Security

После развертывания PT Email Security вы можете выполнить дополнительные действия для первоначальной настройке продукта.

В этом разделе

[Настройка доменного имени PT Email Security \(см. раздел 8.1\)](#)

[Добавление адресов для доступа к веб-интерфейсу PT Email Security \(см. раздел 8.2\)](#)

[Настройка подключения к прокси-серверу \(см. раздел 8.3\)](#)

[Настройка подключения к прокси-серверу с SSL-инспекцией \(см. раздел 8.4\)](#)

[Активация и замена лицензии PT Email Security \(см. раздел 8.5\)](#)

[Подключение внешнего PT MC \(см. раздел 8.6\)](#)

[Установка доверенного SSL-сертификата \(см. раздел 8.7\)](#)

[Отключение передачи информации о работе PT Email Security \(см. раздел 8.8\)](#)

8.1. Настройка доменного имени PT Email Security

Внимание! После подключения доменного имени веб-интерфейс PT Email Security не будет доступен по IP-адресу.

Перед выполнением инструкции вам нужно настроить в сетевой инфраструктуре организации сопоставление выбранного доменного имени с IP-адресом основного узла PT Email Security или с виртуальным IP-адресом службы Keeralived (для конфигураций с отказоустойчивым кластером).

- ▶ Чтобы подключить доменное имя к PT Email Security,

выполните команду:

```
ptmsctl web-interface domain-name apply <Доменное имя>
```

Например:

```
sudo ptmsctl web-interface domain-name apply emailsecurity.example.org
```

Параметры будут применены, появится сообщение `Please wait a few minutes while the system components are restarted.`

- ▶ Чтобы просмотреть подключенное к PT Email Security доменное имя,

выполните команду:

```
sudo ptmsctl web-interface domain-name view
```

Если к PT Email Security подключено доменное имя, то появится сообщение `Domain name connected to the product: <Доменное имя>`. Если доменное имя не подключено, то появится сообщение `No domain name is connected.`

- ▶ Чтобы отключить доменное имя от PT Email Security,

выполните команду:

```
sudo ptmsctl web-interface domain-name reset
```

Параметры будут применены, появится сообщение `Please wait a few minutes while the system components are restarted.`

8.2. Добавление адресов для доступа к веб-интерфейсу PT Email Security

При необходимости вы можете добавить дополнительные IP-адреса или доменные имена для доступа к веб-интерфейсу PT Email Security.

Внимание! Дополнительные адреса не предназначены для подключения источников или доступа к службе публичного API PT Email Security.

Перед выполнением инструкции вам необходимо в сетевой инфраструктуре организации настроить сопоставление дополнительных адресов с IP-адресом основного узла PT Email Security, доменным именем (если оно настроено) или с виртуальным IP-адресом службы Keepalived (для конфигураций с отказоустойчивым кластером).

- ▶ Чтобы добавить дополнительный адрес,

выполните команду:

```
sudo ptmsctl web-interface mc-endpoints add -ep <IP-адрес или доменное имя>:<Порт>
```

Например:

```
sudo ptmsctl web-interface mc-endpoints add -ep 192.0.2.12:555
```

- ▶ Чтобы просмотреть список дополнительных IP-адресов,

выполните команду:

```
sudo ptmsctl web-interface mc-endpoints list
```

- ▶ Чтобы удалить дополнительный IP-адрес,

выполните команду:

```
sudo ptmsctl web-interface mc-endpoints delete -ep <IP-адрес или доменное имя>:<Порт>
```

Например:

```
sudo ptmsctl web-interface mc-endpoints delete -ep 192.0.2.12:555
```

8.3. Настройка подключения к прокси-серверу

Если для доступа к внешним ресурсам в сети организации используется прокси-сервер типа HTTP, необходимо после установки PT Email Security настроить его подключение к прокси-серверу.

Примечание. При использовании прокси-сервера гостевые ОС виртуальных машин, запускаемых для поведенческого анализа файлов, не имеют доступа к внешним сетевым ресурсам. Для настройки доступа на узле с функцией поведенческого анализа необходимо добавить сетевой интерфейс и настроить маршрутизацию трафика виртуальных машин через отдельный шлюз. За инструкцией вы можете обратиться в техническую поддержку Positive Technologies.

Настройка подключения к прокси-серверу

► Чтобы настроить подключение PT Email Security к прокси-серверу:

1. На основном узле выполните команду:

```
sudo ptmsctl product settings apply --proxy-server 'http://<IP-адрес прокси-сервера>:<Порт>' --proxy-user '<Логин>' --proxy-password '<Пароль>'
```

Появится сообщение `Settings applied`.

2. На каждом узле PT Email Security перейдите в каталог с распакованным установщиком и выполните команду:

- Если вы настраиваете основной узел:

```
sudo ./utils/install-k8s.sh --proxy-addr 'http://<IP-адрес прокси-сервера>:<Порт>' --proxy-user '<Логин>' --proxy-pass '<Пароль>'
```

- Если вы настраиваете дополнительный узел:

```
sudo ./utils/install-k8s.sh --slave --proxy-addr 'http://<IP-адрес прокси-сервера>:<Порт>' --proxy-user '<Логин>' --proxy-pass '<Пароль>'
```

Появится сообщение `Kubernetes successfully installed`.

Удаление параметров прокси-сервера

► Чтобы удалить параметры прокси-сервера:

1. На основном узле выполните команду:

```
sudo ptmsctl product settings apply --proxy-server ""
```

Появится сообщение `Settings applied`.

2. На каждом узле PT Email Security перейдите в каталог с распакованным установщиком и выполните команду:

- Если вы настраиваете основной узел:

```
sudo ./utils/install-k8s.sh --no-checks
```

- Если вы настраиваете дополнительный узел:

```
sudo ./utils/install-k8s.sh --slave --no-checks
```

Появится сообщение `Kubernetes successfully installed`.

8.4. Настройка подключения к прокси-серверу с SSL-инспекцией

Для доступа к внешним ресурсам по протоколу HTTPS в сети организации может использоваться прокси-сервер с SSL-инспекцией. Такой прокси-сервер расшифровывает и зашифровывает трафик, используя динамически формируемые сертификаты. Эти сертификаты удостоверяются корневым сертификатом.

Если в сети организации используется прокси-сервер с SSL-инспекцией, для доступа PT Email Security к внешним ресурсам необходимо настроить его подключение к прокси-серверу. Это можно сделать при установке компонентов PT Email Security или после завершения развертывания. При настройке подключения необходимо указать в параметрах PT Email Security адрес прокси-сервера и пользовательский корневой сертификат. Установка пользовательского корневого сертификата также необходима для автоматического обновления PT Email Security. Поддерживаются только сертификаты формата PEM.

Примечание. При использовании прокси-сервера гостевые ОС виртуальных машин, запускаемых для поведенческого анализа файлов, не имеют доступа к внешним сетевым ресурсам. Для настройки доступа на узле с функцией поведенческого анализа необходимо добавить сетевой интерфейс и настроить маршрутизацию трафика виртуальных машин через отдельный шлюз. За инструкцией вы можете обратиться в техническую поддержку Positive Technologies.

Настройка подключения к прокси-серверу при установке компонентов PT Email Security

Вы можете настроить подключение к прокси-серверу с SSL-инспекцией при установке на узле компонентов PT Email Security. Для этого в команде установки необходимо указать параметры `--proxy-addr` '`http://<IP-адрес прокси-сервера>:<Порт>`' `--proxy-ca-crt` '`<Полный путь к файлу корневого сертификата>`'.

Пример команды для установки компонентов PT Email Security на основной узел:

```
sudo ./install.sh --serial-number '...' --proxy-addr 'http://192.0.2.15:3128' --  
proxy-ca-crt '/opt/ptms/user_certs/rootCA.crt'
```

Пример команды для установки компонентов PT Email Security на дополнительный узел:

```
sudo ./k8s-join-node.sh --cluster-ip 192.0.2.55 --token ah93de.ulgb1oah2uofp1kj --  
proxy-addr 'http://192.0.2.15:3128' --proxy-ca-crt '/home/username/rootCA.crt'
```

Настройка подключения к прокси-серверу после развертывания PT Email Security

Вы можете настроить подключение к прокси-серверу с SSL-инспекцией после развертывания PT Email Security. Изменение параметров подключения к прокси-серверу также может потребоваться при изменении его адреса или замене пользовательского корневого сертификата.

- Чтобы настроить подключение PT Email Security к прокси-серверу с SSL-инспекцией:

1. На основном узле выполните команду:

```
sudo ptmsctl product settings apply --proxy-server 'http://<IP-адрес прокси-сервера>:<Порт>' --proxy-ca-crt '<Полный путь к файлу корневого сертификата>'
```

Появится сообщение `Settings applied`.

2. На каждом узле PT Email Security перейдите в каталог с распакованным установщиком и выполните команду:

- Если вы настраиваете основной узел:

```
sudo ./utils/install-k8s.sh --proxy-addr 'http://<IP-адрес прокси-сервера>:<Порт>' --proxy-user '<Логин>' --proxy-pass '<Пароль>' --proxy-ca-crt '<Полный путь к файлу корневого сертификата>'
```

- Если вы настраиваете дополнительный узел:

```
sudo ./utils/install-k8s.sh --slave --proxy-addr 'http://<IP-адрес прокси-сервера>:<Порт>' --proxy-user '<Логин>' --proxy-pass '<Пароль>' --proxy-ca-crt '<Полный путь к файлу корневого сертификата>'
```

Появится сообщение `Kubernetes successfully installed`.

Отключение использования пользовательского корневого сертификата

Если прокси-сервер больше не выполняет SSL-инспекцию трафика, вам необходимо отключить использование пользовательского корневого сертификата.

- Чтобы отключить использование пользовательского корневого сертификата,

на основном узле выполните команду:

```
sudo ptmsctl product settings apply --without-proxy-ca-crt
```

Появится сообщение `Settings applied`.

8.5. Активация и замена лицензии PT Email Security

Если вы не вводили серийный номер лицензии при разворачивании PT Email Security, вам нужно активировать лицензию. Для приобретения лицензии или изменения параметров уже приобретенной лицензии вы можете обратиться в техническую поддержку Positive Technologies.

Примечание. Вы можете узнать информацию об установленной лицензии, выполнив на основном узле PT Email Security команду `sudo ptmsctl license info`.

Для активации лицензии, вам нужно ввести указать серийный номер лицензии в PT Email Security. Серийный номер указывается в файле `serial number.txt` на установочном диске из комплекта поставки или высылается в электронном письме на адрес, указанный при заказе лицензии.

Инструкцию необходимо выполнять на основном узле PT Email Security.

- ▶ Чтобы активировать или заменить лицензию,

выполните команду:

```
sudo ptmsctl license apply --serial-number '<Серийный номер лицензии>'
```

Например:

```
sudo ptmsctl license apply --serial-number 'xxxxxx-xxxxxx-xxxxxx-xxxxxx-xxxxxx-xxxxxx-
xxxxxx-xxxxxx-xxxxxx-xxxxxx'
```

8.6. Подключение внешнего PT MC

Вход пользователей в PT Email Security выполняется с помощью компонента PT MC, который обеспечивает единый механизм аутентификации во всех продуктах Positive Technologies. Данные между PT Email Security и PT MC передаются в зашифрованном виде.

Для входа можно использовать встроенный или внешний PT MC:

- Встроенный PT MC автоматически устанавливается на основной узел PT Email Security при развертывании.

Примечание. Использование встроенного PT MC для входа в другие продукты Positive Technologies не поддерживается.

- Внешний PT MC может быть установлен вместе с другим продуктом Positive Technologies и подключен к PT Email Security.

Внимание! Поддерживается внешний PT MC версии 101.4 или выше.

Для подключения внешнего PT MC вам необходимо:

1. Скопировать на основной узел PT Email Security корневой сертификат, которым подписан сертификат узла внешнего PT MC. Необходимо использовать сертификат в виде файла с расширением .crt.

Примечание. Получить такой сертификат вы можете у администратора внешнего PT MC.

2. На основном узле зарегистрировать PT Email Security во внешнем PT MC.
3. Через веб-интерфейс PT MC подтвердить регистрацию PT Email Security согласно инструкции в технической документации PT MC.

Примечание. Подтверждение регистрации PT Email Security не требуется, если в PT MC отключено подтверждение регистрации приложений или если вы подключаете внешний PT MC версии 101.2 или ниже.

- ▶ Чтобы зарегистрировать PT Email Security во внешнем PT MC,

выполните команду:

```
sudo ptmsctl auth use-remote \
--tenant-internal-url https://<IP-адрес или FQDN внешнего PT MC>:8703 \
--iam-internal-url https://<IP-адрес или FQDN внешнего PT MC>:3334 \
--ca-crt <Путь до сертификата PT MC> \
--ms-name '<Название экземпляра PT Email Security>'
```

Внимание! Использование FQDN с прописными буквами не поддерживается.

Примечание. Если вы планируете регистрировать несколько экземпляров PT Email Security, в параметре `--ms-name` необходимо указать уникальное название экземпляра. Если вы планируете регистрировать только один экземпляр, параметр можно опустить.

Например:

```
sudo ptmsctl auth use-remote \
--tenant-internal-url https://ptmc.example:8703 \
--iam-internal-url https://ptmc.example:3334 \
--ca-crt /home/user/MC_RootCA.crt \
--ms-name 'PT Email Security'
```

Компоненты PT Email Security будут перезапущены.

- ▶ Чтобы подключить встроенный PT MC,

выполните команду:

```
sudo ptmsctl auth use-local
```

8.7. Установка доверенного SSL-сертификата

Для доступа пользователей к веб-интерфейсу PT Email Security через HTTPS-соединение можно использовать SSL-сертификат доверенного центра сертификации вашей организации. Для этого SSL-сертификат необходимо установить в PT Email Security.

SSL-сертификат должен соответствовать следующим требованиям:

- используется алгоритм подписи SHA-256;
- для шифрования ключей используется алгоритм RSA;
- длина закрытого ключа — не менее 2048 бит;
- включает область применения сертификата Digital Signature или Key Encipherment;
- в расширении Subject Alternative Name (SAN) указаны: IP-адрес основного узла PT Email Security, доменное имя основного узла (если оно подключено) и IP-адрес службы Keeralived (если настроена конфигурация с отказоустойчивым кластером).

Устанавливать SSL-сертификат необходимо на основном узле PT Email Security. Для установки SSL-сертификата на основном узле должны быть доступны:

- файл открытого ключа SSL-сертификата;
- файл закрытого ключа, который расшифрован без SSL-сертификата в нем;
- файл `.pem` сертификата издателя, выпустившего SSL-сертификат.

- ▶ Чтобы установить доверенный SSL-сертификат в PT Email Security,

выполните команду:

```
sudo ptmsctl web-interface https-certs apply --crt <Файл открытого ключа SSL-сертификата>
--key <Файл закрытого ключа> --ca-bundle <Файл .pem сертификата издателя>
```

Например:

```
sudo ptmsctl web-interface https-certs apply --crt /home/user/your_company.crt --key /home/user/your_company.key --ca-bundle /etc/ssl/certs/root_ca.pem
```

Параметры будут применены, появится сообщение `Please wait a few minutes while the system components are restarted.`

Доверенный SSL-сертификат установлен.

8.8. Отключение передачи информации о работе PT Email Security

PT Email Security собирает и передает в Positive Technologies следующую информацию о заданиях на проверку объектов:

- Идентификаторы заданий.
- Данные о поступивших на проверку файлах (имя, размер, MIME-тип, хеш-суммы).
- Информацию об используемых средствах проверки и антивирусах (название, версия, примененное правило).
- Информацию об используемых при проверке образах виртуальных машин.
- Результат проверки (название и класс обнаруженного вредоносного ПО).

Эта информация необходима для повышения качества экспертизы и дальнейшего развития PT Email Security. Вся информация передается в обезличенном и зашифрованном виде.

Если политика информационной безопасности вашей организации запрещает передачу такой информации в сторонние компании, вы можете отключить передачу информации. Для получения инструкций обратитесь в техническую поддержку Positive Technologies.

9. Изменение конфигурации PT Email Security

Вы можете изменять конфигурацию PT Email Security, добавляя и удаляя дополнительные узлы для поведенческого анализа файлов.

Например, если в базовой конфигурации PT Email Security вам нужно уменьшить время проверки файлов, вы можете добавить в конфигурацию дополнительные узлы, отключить на основном узле функцию поведенческого анализа и получить тем самым высоконагруженную конфигурацию PT Email Security.

Для добавления дополнительного узла в конфигурацию PT Email Security вам необходимо:

1. Развернуть дополнительные узлы [с помощью установщика \(см. раздел 7.3\)](#).
2. На дополнительных узлах активировать функцию поведенческого анализа.
3. На основном узле отключить функцию поведенческого анализа.
4. Удалить с основного узла гипервизор Xen.

Если в высоконагруженной конфигурации PT Email Security требуется переустановить дополнительный узел или перенести его на другой физический сервер, сперва необходимо удалить дополнительный узел из конфигурации PT Email Security, а затем заново развернуть его на том же или другом сервере.

Примечание. Если дополнительный узел вышел из строя, достаточно на основном узле исключить его из конфигурации PT Email Security.

Для удаления дополнительного узла из конфигурации PT Email Security вам необходимо:

1. На основном узле исключить дополнительный узел из конфигурации PT Email Security.
2. Удалить с дополнительного узла компоненты PT Email Security.
3. Удалить с дополнительного узла гипервизор Xen.

В этом разделе

[Исключение дополнительного узла из конфигурации PT Email Security \(см. раздел 9.1\)](#)

[Удаление с узла гипервизора Xen \(см. раздел 9.2\)](#)

[Удаление с узла компонентов PT Email Security \(см. раздел 9.3\)](#)

9.1. Исключение дополнительного узла из конфигурации PT Email Security

Инструкцию необходимо выполнять на основном узле PT Email Security.

- Чтобы исключить дополнительный узел из конфигурации PT Email Security:

1. Получите список узлов PT Email Security:

```
sudo kubectl --kubeconfig /etc/kubernetes/admin.conf get node
```

2. Если дополнительный узел указан в списке, исключите его из конфигурации:

```
sudo kubectl --kubeconfig /etc/kubernetes/admin.conf delete node <Имя дополнительного узла>
```

Появится сообщение об удалении дополнительного узла.

9.2. Удаление с узла гипервизора Xen

- Чтобы удалить с узла гипервизор Xen:

1. Перейдите в каталог со скриптами установщика PT Email Security:

```
cd /home/user/ptsb-installer
```

2. Запустите скрипт `purge.sh`:

```
sudo xen/purge.sh
```

3. По завершении работы скрипта нажмите клавишу Enter.

Узел будет перезагружен.

Гипервизор Xen удален с узла.

9.3. Удаление с узла компонентов PT Email Security

- Чтобы удалить с узла компоненты PT Email Security:

1. Перейдите в каталог со скриптами установщика PT Email Security:

```
cd /home/user/ptsb-installer
```

2. Запустите скрипт `purge-kubernetes.sh`:

```
sudo ./purge-kubernetes.sh
```

3. По завершении работы скрипта нажмите клавишу Enter.

Узел будет перезагружен.

Компоненты PT Email Security удалены с узла.

10. О технической поддержке

Гарантийная поддержка доступна для всех владельцев действующих лицензий на PT Email Security в течение периода предоставления обновлений и включает в себя следующий набор услуг.

Предоставление доступа к обновленным версиям продукта

Обновления продукта выпускаются в порядке и в сроки, определяемые Positive Technologies. Positive Technologies предоставляет обновленные версии продукта в течение оплаченного периода получения обновлений, указанного в бланке лицензии приобретенного продукта Positive Technologies.

Positive Technologies не производит установку обновлений продукта в рамках гарантийной поддержки и не несет ответственности за инциденты, возникшие в связи с некорректной или несвоевременной установкой обновлений продукта.

Восстановление работоспособности продукта

Специалист Positive Technologies проводит диагностику заявленного сбоя и предоставляет рекомендации для восстановления работоспособности продукта. Восстановление работоспособности может заключаться в выдаче рекомендаций по установке продукта заново с потенциальной потерей накопленных данных либо в восстановлении версии продукта из доступной резервной копии (резервное копирование должно быть настроено заблаговременно). Positive Technologies не несет ответственности за потерю данных в случае неверно настроенного резервного копирования.

Примечание. Помощь оказывается при условии, что конечным пользователем продукта соблюдены все аппаратные, программные и иные требования и ограничения, описанные в документации к продукту.

Устранение ошибок и дефектов в работе продукта в рамках выпуска обновленных версий

Если в результате диагностики обнаружен дефект или ошибка в работе продукта, Positive Technologies обязуется включить исправление в ближайшие возможные обновления продукта (с учетом релизного цикла продукта, приоритета дефекта или ошибки, сложности требуемых изменений, а также экономической целесообразности исправления). Сроки выпуска обновлений продукта остаются на усмотрение Positive Technologies.

Рассмотрение предложений по доработке продукта

При обращении с предложением по доработке продукта необходимо подробно описать цель такой доработки. Вы можете поделиться рекомендациями по улучшению продукта и оптимизации его функциональности. Positive Technologies обязуется рассмотреть все предложения, однако не принимает на себя обязательств по реализации каких-либо

доработок. Если Positive Technologies принимает решение о доработке продукта, то способы ее реализации остаются на усмотрение Positive Technologies. Заявки принимаются [на портале технической поддержки](#).

Портал технической поддержки

[На портале технической поддержки](#) вы можете круглосуточно создавать и обновлять заявки и читать новости продуктов.

Для получения доступа к portalу технической поддержки нужно создать учетную запись, используя адрес электронной почты в официальном домене вашей организации. Вы можете указать другие адреса электронной почты в качестве дополнительных. Добавьте в профиль название вашей организации и контактный телефон — так нам будет проще с вами связаться.

Поддержка на портале предоставляется на русском и английском языках.

Условия предоставления гарантийной поддержки

Для получения гарантийной поддержки необходимо оставить заявку [на портале технической поддержки](#) и предоставить следующие данные:

- номер лицензии на использование продукта;
- файлы журналов и наборы диагностических данных, которые требуются для анализа;
- снимки экрана.

Positive Technologies не берет на себя обязательств по оказанию услуг гарантийной поддержки в случае вашего отказа предоставить запрашиваемую информацию или отказа от внедрения предоставленных рекомендаций.

Если заказчик не предоставляет необходимую информацию по прошествии 20 календарных дней с момента ее запроса, специалист технической поддержки имеет право закрыть заявку. Оказание услуг может быть возобновлено по вашей инициативе при условии предоставления запрошенной ранее информации.

Услуги по гарантийной поддержке продукта не включают в себя услуги по переустановке продукта, решению проблем с операционной системой, инфраструктурой заказчика или сторонним программным обеспечением.

Заявки могут направлять уполномоченные сотрудники заказчика, владеющего продуктом на законном основании (включая наличие действующей лицензии). Специалисты заказчика должны иметь достаточно знаний и навыков для сбора и предоставления диагностической информации, необходимой для решения заявленной проблемы.

Услуги по гарантийной поддержке оказываются в отношении поддерживаемых версий продукта. Информация о поддерживаемых версиях содержится в «Политике поддержки версий программного обеспечения» и (или) иных информационных материалах, размещенных на официальном веб-сайте Positive Technologies.

Время реакции и приоритизация заявок

При получении заявки ей присваивается регистрационный номер, специалист службы технической поддержки классифицирует ее (присваивает тип и уровень значимости) и выполняет дальнейшие шаги по ее обработке.

Время реакции рассчитывается с момента получения заявки до первичного ответа специалиста технической поддержки с уведомлением о взятии заявки в работу. Время реакции зависит от уровня значимости заявки. Специалист службы технической поддержки оставляет за собой право переопределить уровень значимости в соответствии с приведенными ниже критериями. Указанные сроки являются целевыми, но возможны отклонения от них по объективным причинам.

Таблица 16. Время реакции на заявку

Уровень значимости заявки	Критерии значимости заявки	Время реакции на заявку
Критический	Аварийные сбои, приводящие к невозможности штатной работы продукта (исключая первоначальную установку) либо оказывающие критически значимое влияние на бизнес заказчика	До 4 часов
Высокий	Сбои, проявляющиеся в любых условиях эксплуатации продукта и оказывающие значительное влияние на бизнес заказчика	До 8 часов
Средний	Сбои, проявляющиеся в специфических условиях эксплуатации продукта либо не оказывающие значительного влияния на бизнес заказчика	До 8 часов
Низкий	Вопросы информационного характера либо сбои, не влияющие на эксплуатацию продукта	До 8 часов

Указанные часы относятся к рабочему времени (рабочие дни с 9:00 до 18:00 UTC+3) специалистов технической поддержки. Под рабочим днем понимается любой день за исключением субботы, воскресенья и дней, являющихся официальными нерабочими днями в Российской Федерации.

Обработка и закрытие заявок

По мере рассмотрения заявки и выполнения необходимых действий специалист службы поддержки сообщает вам:

- о ходе диагностики по заявленной проблеме и ее результатах;
- планах выпуска обновленной версии продукта (если требуется для устранения проблемы).

Если по итогам обработки заявки необходимо внести изменения в продукт, Positive Technologies включает работы по исправлению в ближайшее возможное плановое обновление продукта (с учетом релизного цикла продукта, приоритета дефекта или ошибки, сложности требуемых изменений, а также экономической целесообразности исправления). Сроки выпуска обновлений продукта остаются на усмотрение Positive Technologies.

Специалист закрывает заявку, если:

- предоставлены решение или возможность обойти проблему, не влияющие на критически важную функциональность продукта (по усмотрению Positive Technologies);
- диагностирован дефект продукта, собрана техническая информация о дефекте и условиях его воспроизведения, исправление дефекта запланировано к выходу в рамках планового обновления продукта;
- заявленная проблема вызвана программным обеспечением или оборудованием сторонних производителей, на которые не распространяются обязательства Positive Technologies;
- заявленная проблема классифицирована специалистами Positive Technologies как неподдерживаемая.

Примечание. Если продукт приобретался вместе с аппаратной платформой в виде программно-аппаратного комплекса (ПАК), решение заявок, связанных с ограничением или отсутствием работоспособности аппаратных компонентов, происходит согласно условиям и срокам, указанным в гарантийных обязательствах (гарантийных талонах) на такие аппаратные компоненты.



Positive Technologies — один из лидеров в области результативной кибербезопасности. Компания является ведущим разработчиком продуктов, решений и сервисов, позволяющих выявлять и предотвращать кибератаки до того, как они причинят неприемлемый ущерб бизнесу и целым отраслям экономики. Positive Technologies — первая и единственная компания из сферы кибербезопасности на Московской бирже (MOEX: POSI). Количество акционеров превышает 220 тысяч.



Email Security

версия 5.30

Руководство администратора

© Positive Technologies, 2026.

Настоящий документ является собственностью Positive Technologies и защищен законодательством Российской Федерации и международными соглашениями об авторских правах и интеллектуальной собственности.

Копирование документа либо его фрагментов в любой форме, распространение, в том числе в переводе, а также их передача третьим лицам возможны только с письменного разрешения Positive Technologies.

Документ может быть изменен без предварительного уведомления.

Товарные знаки, использованные в тексте, приведены исключительно в информационных целях, исключительные права на них принадлежат соответствующим правообладателям.

Дата редакции документа: 06.02.2026

Содержание

1.	Об этом документе.....	5
1.1.	Условные обозначения.....	5
1.2.	Другие источники информации о PT Email Security.....	6
2.	О PT Email Security.....	7
3.	Компоненты PT Email Security.....	9
4.	Требования к рабочим станциям.....	10
5.	Настройка аутентификации.....	11
6.	Вход в PT Email Security.....	14
7.	Интерфейс PT Email Security.....	15
8.	Лицензирование.....	18
9.	Настройка средств проверки.....	21
9.1.	Настройка средств проверки Positive Technologies.....	21
9.2.	Настройка антивирусов.....	25
9.3.	Настройка поведенческого анализа.....	29
9.4.	Работа с пользовательскими YARA-правилами.....	30
10.	Настройка основных параметров PT Email Security.....	31
11.	Работа с токенами доступа.....	37
12.	Работа с источниками.....	39
12.1.	Настройка источников.....	42
12.2.	Настройка правил маршрутизации проверенных писем.....	44
12.3.	Отключение автоматической смены режимов проверки.....	47
13.	Подключение источников.....	48
13.1.	Служба Checkme.....	49
13.2.	Общая папка.....	50
13.3.	Папка-шлюз.....	52
13.4.	S3-хранилище.....	54
13.5.	Внешняя система как ICAP-клиент.....	56
13.6.	Внешняя система через API.....	58
13.7.	Почтовый шлюз безопасности.....	60
13.7.1.	Добавление источника в PT Email Security.....	60
13.7.2.	Развертывание почтового шлюза безопасности.....	62
13.7.3.	Добавление правил маршрутизации проверенных писем.....	65
13.7.4.	Добавление доверенных сертификатов.....	67
13.7.5.	Включение проверки адресов получателей.....	68
13.8.	«Код безопасности», «Континент» 4.1.....	68
13.9.	Exim 4 в режиме фильтрации.....	72
13.10.	Exim 4 в режиме зеркалирования.....	79
13.11.	Microsoft Exchange 2010–2019 с установленным почтовым агентом.....	81
13.12.	Microsoft Exchange 2010–2019 в режиме зеркалирования.....	84
13.13.	Postfix 3.2 в режиме фильтрации.....	86
13.14.	Postfix 3.2 в режиме зеркалирования.....	93
13.15.	PT Threat Analyzer 2.10 и выше.....	96
13.16.	Squid 3 и выше.....	97

13.17.	UserGate NGFW 6, 7.1, 7.4	100
14.	Интеграция с внешними системами	105
14.1.	MaxPatrol EDR 6.0 и выше.....	105
14.2.	MaxPatrol SIEM 6.1 и выше.....	106
14.3.	PT AF 3, 4.2.1 и выше	107
14.4.	PT ISIM 5.2 и выше	109
14.5.	PT NAD 7.1 и выше	110
14.6.	PT NGFW 1.8 и выше	111
14.7.	PT Threat Analyzer 2.10 и выше	113
15.	Настройка обновления PT Email Security.....	115
16.	Просмотр конфигурации PT Email Security.....	119
17.	Мониторинг системных ресурсов в Grafana	123
18.	Смена IP-адреса узла PT Email Security	128
19.	Смена DNS-сервера	131
20.	Резервное копирование и восстановление параметров PT Email Security.....	132
21.	Обновление гипервизора Xen	134
22.	Удаление PT Email Security	137
23.	Диагностика и устранение неисправностей.....	138
24.	О технической поддержке.....	141
	Приложение. Сценарии отказов	145
	Глоссарий.....	146

1. Об этом документе

Руководство администратора содержит справочную информацию и инструкции по настройке и администрированию Positive Technologies Email Security (далее также — PT Email Security). Руководство не содержит инструкций по использованию основных функций продукта.

Руководство адресовано специалистам, выполняющим настройку и администрирование PT Email Security.

Комплект документации PT Email Security включает в себя следующие документы:

- Этот документ.
- Руководство по внедрению — содержит информацию для внедрения продукта в инфраструктуре организации: от описания типовых конфигураций до инструкций по установке и первоначальной настройке продукта.
- Руководство специалиста по безопасности — содержит сценарии использования продукта для управления событиями информационной безопасности.
- Руководство пользователя — содержит инструкции по отправке файлов на проверку через интерфейс продукта или по электронной почте и просмотру результатов проверки.
- Руководство разработчика — содержит информацию для интеграции PT Email Security со сторонними системами.

В этом разделе

[Условные обозначения \(см. раздел 1.1\)](#)

[Другие источники информации о PT Email Security \(см. раздел 1.2\)](#)

1.1. Условные обозначения

В документе приняты условные обозначения.

Таблица 1. Условные обозначения

Пример	Описание
Внимание! При выключении модуля снижается уровень защищенности сети	Предупреждения. Содержат информацию о действиях или событиях, которые могут иметь нежелательные последствия
Примечание. Вы можете создать дополнительные отчеты	Примечания. Содержат советы, описания важных частных случаев, дополнительную или справочную информацию, которая может быть полезна при работе с продуктом
► Чтобы открыть файл:	Начало инструкции выделено специальным значком
Нажмите ОК	Названия элементов интерфейса (например, кнопок, полей, пунктов меню) выделены полужирным шрифтом

Пример	Описание
Выполните команду <code>Stop-Service</code>	Текст командной строки, примеры кода, прочие данные, которые нужно ввести с клавиатуры, выделены специальным шрифтом. Также выделены специальным шрифтом имена файлов и пути к файлам и папкам
<code>Ctrl+Alt+Delete</code>	Комбинация клавиш. Чтобы использовать комбинацию, клавиши нужно нажимать одновременно
<Название программы>	Переменные заключены в угловые скобки

1.2. Другие источники информации о PT Email Security

Вы можете найти дополнительную информацию о PT Email Security [на портале технической поддержки](#).

Портал содержит статьи базы знаний, новости обновлений продуктов Positive Technologies, ответы на часто задаваемые вопросы пользователей. Для доступа к базе знаний и всем новостям нужно создать на портале учетную запись.

Если вы не нашли нужную информацию или решение проблемы самостоятельно, обратитесь [в службу технической поддержки \(см. раздел 24\)](#).

2. О PT Email Security

Positive Technologies Email Security (PT Email Security) — система многоуровневой защиты от угроз электронной почты с функциями почтового шлюза и почтового транспортного агента. В системе применяются различные средства статического и динамического анализа объектов, включая антифишинг- и антиспам-проверку, антивирусное сканирование, репутационный, ретроспективный и поведенческий анализ.

PT Email Security предназначен для выявления вредоносных объектов, предотвращения их проникновения и распространения в IT-инфраструктуре организации. Многоуровневая проверка позволяет повысить вероятность обнаружения объектов с угрозами.

PT Email Security может использоваться специалистами по информационной безопасности, администраторами и аналитиками SOC для анализа подозрительных объектов и расследования инцидентов информационной безопасности.

PT Email Security предоставляет следующие основные возможности:

- Инструменты для работы с письмами:
 - Почтовый шлюз безопасности с фильтрацией подключений.
 - Встроенный почтовый транспортный агент.
 - Обработка писем в зависимости от отправителя и получателей.
 - Обезвреживание писем с угрозами.
 - Карантин для подозрительных писем.
- Многоуровневая проверка объектов с использованием методов статического и динамического анализа:
 - Поведенческий анализ файлов в различных операционных системах.
 - Антивирусная проверка файлов.
 - Проверка файлов по YARA-правилам, разработанным специалистами экспертного центра Positive Technologies.
 - Проверка файлов и ссылок по индикаторам компрометации.
 - Антифишинг- и антиспам-проверка писем.
 - Проверка адресов в письмах по спискам DNS-блокировок.
 - Ретроспективный анализ файлов в хранилище.
- Настраиваемые пользователем средства проверки:
 - Черный и белый списки файлов.
 - Проверка файлов по пользовательским YARA-правилам.
 - Пользовательские правила определения файлов и ссылок с угрозами.

- Экспертные инструменты для проверки объектов и расследования инцидентов:
 - Гибкий поиск заданий и объектов с использованием языка запросов QL.
 - Проверка объектов по базам VirusTotal и PT IoC Portal.
 - Поведенческий анализ файлов в интерактивном режиме.
 - Диаграммы поведенческого анализа.
- Быстрая проверка объектов через веб-интерфейс или по электронной почте.
- Поточковая проверка объектов, поступающих из различных источников:
 - Почтовый трафик серверов электронной почты с возможностью блокировки писем с угрозами.
 - Объекты от ICAP-клиентов с возможностью блокировки объектов с угрозами.
 - Объекты из файловых хранилищ и файловых шлюзов.
 - Объекты, передаваемые через публичный API PT Email Security.
- Интеграция с продуктами Positive Technologies:
 - MaxPatrol EDR.
 - MaxPatrol SIEM.
 - PT AF.
 - PT ISIM.
 - PT NAD.
 - PT NGFW.
 - PT Threat Analyzer.

PT Email Security также предоставляет дополнительные возможности:

- Мониторинг проверки объектов и обнаруженных угроз.
- Отправка почтовых уведомлений об угрозах.
- Управление очередью файлов, направляемых на поведенческий анализ.
- Управление приоритетами источников и типов файлов при поведенческом анализе.
- Формирование отчетов по заданиям и проверенным объектам.
- Скачивание проверенных файлов из хранилища.
- Мониторинг работы PT Email Security в Grafana с возможностью отправки почтовых уведомлений.

3. Компоненты PT Email Security

В состав PT Email Security входят следующие компоненты:

- Встроенный PT MC — компонент, отвечающий за аутентификацию и авторизацию пользователей PT Email Security (пользовательские данные хранятся в базе данных под управлением СУБД PostgreSQL).

Примечание. При использовании встроенного PT MC не рекомендуется интегрировать его с другими площадками в иерархии и не рекомендуется подключать к нему другие продукты.

Примечание. Встроенный PT MC может быть заменен на внешний экземпляр.

- Веб-интерфейс — компонент графического пользовательского интерфейса PT Email Security, доступный в браузере.
- Ядро проверки — компонент, который отправляет объекты на проверку и контролирует выполнение проверки.
- Модуль поведенческого анализа — компонент, отвечающий за проверку файлов методом поведенческого анализа.
- Хранилище файлов — компонент, отвечающий за хранение полученных извне файлов на жестком диске.
- База данных — компонент под управлением СУБД ClickHouse, который обеспечивает хранение данных о заданиях и файлах.
- API базы данных — компонент, который обеспечивает отображение информации из базы данных в веб-интерфейсе PT Email Security.
- Служба Updater — компонент, который обеспечивает скачивание и установку обновлений PT Email Security и образов VM. Включает в себя функции работы с лицензией продукта.
- Служба высокой доступности Keeralived — компонент, который обеспечивает доступность всех узлов отказоустойчивого кластера PT Email Security на одном IP-адресе.

4. Требования к рабочим станциям

К рабочим станциям администраторов PT Email Security, выдвигаются следующие аппаратные и программные требования:

- Разрешение монитора — Full HD (не менее 1920 × 1080 пикселей).
- Браузер — Google Chrome версии 140, Microsoft Edge 140, Mozilla Firefox 142, Yandex Browser 25.8 или более новых версий.
- На узле должны быть разрешены исходящие подключения к портам TCP 22, 80, 443, 3334, 8703, 8704.
- Если на узле установлен антивирус:
 - В исключения антивируса должны быть добавлены правила, которые разрешают доступ к основному узлу PT Email Security и используемым прокси-серверам по протоколам HTTP и HTTPS.
 - В PT Email Security должен быть установлен пользовательский SSL-сертификат, выпущенный доверенным центром сертификации.

5. Настройка аутентификации

Вход пользователей в PT Email Security выполняется с помощью компонента PT MC, который обеспечивает единый механизм аутентификации во всех продуктах Positive Technologies. Может использоваться встроенный или внешний PT MC.

Для входа в PT MC используется адрес вида `https://<Адрес PT Email Security>:3334`.

При этом в качестве адреса PT Email Security необходимо указать:

- Если установлена конфигурация с отказоустойчивым кластером, — виртуальный IP-адрес службы Keeralived.
- Если установлена другая конфигурация PT Email Security, — IP-адрес основного узла.

Для первого входа в PT MC используется стандартная учетная запись суперпользователя `Administrator` с паролем `P@ssw0rd`. Это учетная запись предоставляет неограниченные права в PT Email Security и встроенном PT MC.

Внимание! В целях безопасности сразу после первого входа в PT MC вам необходимо сменить пароль учетной записи суперпользователя.

Создание учетных записей для пользователей PT Email Security и назначение им ролей необходимо выполнять согласно инструкциям в технической документации PT MC. Если вы используете встроенный PT MC, следуйте инструкциям для версии 101.12, если был подключен внешний PT MC, используйте инструкции для подключенной версии.

Настройка аутентификации по LDAP

В PT MC поддерживается два типа аутентификации пользователей: локальный и по протоколу LDAP. Для каждого пользователя может быть выбран свой тип аутентификации. По умолчанию используется только локальная аутентификация.

При локальной аутентификации все данные о пользователях, включая их логины и пароли, хранятся в PT MC. При LDAP-аутентификации логины и пароли пользователей хранятся в Microsoft Active Directory. Персональная и организационная информация по умолчанию также загружается из Microsoft Active Directory, но может быть указана и изменена в PT MC.

Для использования LDAP-аутентификации вам нужно согласно инструкциям в технической документации PT MC настроить подключение к одному или нескольким LDAP-серверам вашей организации и при необходимости настроить синхронизацию с Microsoft Active Directory.

Если вы используете встроенный PT MC и связь с LDAP-сервером должна осуществляться через зашифрованное соединение (LDAP по SSL, или LDAPS), на основном узле PT Email Security вам необходимо установить доверенный сертификат корневого центра сертификации, используемый этим LDAP-сервером. Получить такой сертификат вы можете у администратора контроллера домена.

Внимание! Необходимо использовать сертификат в виде файла X.509 в кодировке Base64.

- Чтобы установить доверенный сертификат для LDAPS,

выполните команду:

```
sudo ptmsctl auth use-local --ldaps-ca-crt <Путь к файлу сертификата>
```

Примечание. Повторное выполнение команды заменяет ранее установленный сертификат.

Например:

```
sudo ptmsctl auth use-local --ldaps-ca-crt /home/user/certificate_ca.crt
```

Доверенный сертификат для LDAPS установлен.

Роли пользователей

Для учетных записей пользователей PT Email Security используется ролевая модель управления доступом. Предусмотрены следующие стандартные роли: администратор, специалист по безопасности и пользователь. Доступные для каждой роли привилегии и страницы PT Email Security указаны в таблице.

Примечание. При создании учетной записи можно назначить ей одновременно несколько ролей. Например, вы можете создать еще одну учетную запись суперпользователя, назначив ей все три роли.

Таблица 2. Доступные для пользователей страницы и привилегии

Страницы и привилегии	Роль пользователя		
	Администратор	Специалист по безопасности	Пользователь
Получение системных уведомлений	Да	—	—
Получение уведомлений безопасности	—	Да	—
Страница Сводка	—	Да	—
Просмотр сводки	—	Да	—
Страница Задания	Да	Да	Да
Создание заданий на проверку	Да	Да	Да
Доступ к своим результатам проверки	Да	Да	Да
Доступ ко всем результатам проверки	—	Да	—
Страница Объекты	Да	Да	Да
Просмотр информации о файле	Да	Да	Да
Управление метками и комментариями к файлам	Да	Да	Да
Просмотр списка всех файлов	—	Да	—

Страницы и привилегии	Роль пользователя		
	Администратор	Специалист по безопасности	Пользователь
Просмотр истории проверки файла	—	Да	—
Скачивание файлов	—	Да	—
Страница Экспертиза РТ	Да	Да	—
Страница Антивирусы	Да	Да	—
Просмотр информации об антивирусах	Да ¹	Да	—
Просмотр статистики антивирусов	—	Да	—
Страница Образы ВМ	—	Да	—
Страница Черный список	—	Да	—
Страница Белый список	—	Да	—
Страница Источники	Да	Да	—
Изменение параметров проверки	—	Да	—
Страница Основные параметры	Да	Да	—
Мониторинг текущего состояния системы	Да	Да	—
Изменение параметров системы	Да	—	—
Страница Токены доступа	Да	Да	—
Страница Обновления	Да	—	—
Страница Конфигурация	Да	Да	—
Страница Лицензия	Да	—	—

¹ Доступна установка дополнительных средств проверки.

6. Вход в PT Email Security

Вход в PT Email Security выполняется с помощью компонента PT MC, который обеспечивает единый механизм входа в продукты Positive Technologies.

Для входа в PT Email Security вам понадобится адрес веб-интерфейса PT Email Security и данные учетной записи.

► Чтобы войти в PT Email Security:

1. В адресной строке браузера введите адрес веб-интерфейса PT Email Security и нажмите клавишу Enter.

Откроется страница входа в PT Email Security или страница для анонимной проверки объектов.

2. Нажмите кнопку **Войти**.

Откроется страница входа в PT MC.

3. Если вы используете доменную учетную запись, выберите вкладку **LDAP**.

4. Введите данные учетной записи.

5. Нажмите кнопку **Войти**.

Откроется веб-интерфейс PT Email Security.

7. Интерфейс PT Email Security

Работа с PT Email Security выполняется через веб-интерфейс. Все передаваемые при работе данные защищаются при помощи HTTPS с использованием SSL-сертификата. Сертификат может быть как самоподписанным, так и выданным официальным центром сертификации.

Главное меню

Для доступа пользователей к страницам веб-интерфейса и основным функциям PT Email Security используется главное меню. В главном меню расположены следующие элементы управления.

 — кнопка для перехода между приложениями Positive Technologies, которые зарегистрированы в сервисе управления пользователями и доступом PT MC.

Разделы для перехода к страницам веб-интерфейса:

- **Задания** — для работы с заданиями на проверку объектов.
- **Объекты** — для работы с объектами в хранилище.
- **Средства проверки** — содержит пункты для перехода к следующим страницам:
 - **Экспертиза PT** — для работы со средствами проверки, которые разработаны специалистами Positive Technologies.
 - **Антивирусы** — для работы с антивирусами сторонних разработчиков, которые используются при проверке файлов.
 - **Пользовательские правила** — для работы со средством проверки объектов по пользовательским YARA-правилам.
- **Источники** — для работы с источниками, от которых поступают объекты на проверку.
- **Система** — содержит пункты для перехода к следующим страницам:
 - **Основные параметры** — для настройки основных параметров работы PT Email Security.
 - **Токены доступа** — для работы с токенами для доступа к PT Email Security через публичный API.
 - **Обновления** — для работы с обновлениями PT Email Security.
 - **Конфигурация** — содержит пункты для перехода к страницам с информацией о настроенной конфигурации, компонентах, узлах и подах PT Email Security, а также для мониторинга системных ресурсов узлов с помощью средства визуализации и мониторинга данных Grafana.
 - **Лицензия** — для работы с лицензией PT Email Security.

Проверить объекты — кнопка для проверки объектов через веб-интерфейс.

Также в главном меню расположены значки:

 — для просмотра уведомлений о проверке объектов, отправленных вами через интерфейс. На значке отображается количество проверенных объектов. По ссылке в уведомлении вы можете открыть карточку задания, в котором проверен объект.

 — для просмотра уведомлений о работе компонентов PT Email Security и доступных обновлениях. На значке отображается количество новых уведомлений. При нажатии на значок вы можете:

- Посмотреть версию PT Email Security.
- Скачать файлы журналов PT Email Security.
- Перейти на сайт технической поддержки Positive Technologies.

 — для просмотра логина, под которым вы вошли в PT Email Security. При нажатии на значок вы можете:

- Сменить тему оформления и язык интерфейса.
- Выйти из PT Email Security.

Смена языка и темы оформления интерфейса

Интерфейс PT Email Security доступен на русском и английском языках в светлой и темной темах оформления. По умолчанию выбраны русский язык и светлая тема.

► Чтобы сменить язык интерфейса,

в главном меню выберите  → **Язык** → **<Название языка>**.

► Чтобы сменить тему интерфейса,

в главном меню выберите  → **Тема** → **<Название темы>**.

Примечание. Для выбора темы, соответствующей оформлению интерфейса ОС, вы можете выбрать **Системная**.

Аудит действий пользователей

В PT Email Security реализован аудит действий пользователей. Регистрируются события безопасности, связанные со следующими действиями пользователей:

- просмотр заданий;
- скачивание результатов проверки и файлов из хранилища;
- очистка очереди файлов на поведенческий анализ;
- просмотр и выпуск писем из карантина;
- изменение параметров проверки источников;

- работа с источниками (добавление, удаление, включение, отключение и изменение параметров);
- работа с антивирусами и (установка, удаление, включение и отключение);
- работа со средствами проверки Positive Technologies (включение, отключение и изменение параметров);
- работа с черным и белым списками (очистка, скачивание);
- работа с записями в черном и белом списках (добавление, удаление, перемещение между списками, добавление комментариев);
- работа с токенами доступа (создание, добавление комментария, привязка к источнику и отзыв);
- работа с образами виртуальных машин (добавление, удаление и скачивание);
- скачивание файлов журналов;
- изменение основных параметров PT Email Security;
- запуск обновления PT Email Security и изменение параметров автоматического обновления;
- замена лицензии PT Email Security.

Кроме того, регистрируются события безопасности, связанные со следующими автоматическими действиями PT Email Security:

- обновление PT Email Security по расписанию;
- обновление антивирусов, антивирусных баз, средств проверки Positive Technologies и их баз знаний.

Все зарегистрированные события отображаются в журнале действий PT MC.

8. Лицензирование

Чтобы использовать PT Email Security, вам нужно приобрести и активировать лицензию. Для приобретения лицензии или изменения параметров уже приобретенной лицензии вы можете обратиться в техническую поддержку Positive Technologies.

Если вы не вводили серийный номер лицензии при установке PT Email Security, вам нужно активировать лицензию после установки.

Чтобы активировать лицензию, приобретенную вашей организацией, вам нужно ввести серийный номер этой лицензии в интерфейсе PT Email Security. Серийный номер указывается в файле `serial number.txt` на установочном диске из комплекта поставки или высылается в электронном письме на адрес, указанный при заказе лицензии.

Замена лицензии может потребоваться в следующих случаях:

- Одна и та же лицензия была активирована в нескольких экземплярах PT Email Security. Поскольку одна лицензия может использоваться только в одном экземпляре продукта, вам нужно заменить лицензии так, чтобы в каждом экземпляре была активирована своя лицензия.

Примечание. При нехватке лицензий вашей организации нужно докупить их.

- Лицензия была активирована не в том экземпляре PT Email Security. Например, лицензия, которая позволяет проверять только почтовый трафик организации, была активирована в экземпляре, который вы устанавливали исключительно для самостоятельной проверки файлов пользователями.
- Конфигурация сервера с установленным PT Email Security менялась более трех раз (например, заменялись комплектующие сервера), вследствие чего лицензия стала недействительной. В таком случае вам нужно обратиться в техническую поддержку Positive Technologies для получения новой лицензии с теми же параметрами.

Управление лицензией осуществляется на странице **Система** → **Лицензия**.

↔ Заменить лицензию

↺ Проверить лицензию

Проверена 12 февраля, 10:58

Лицензия

№ 4 · Bn4s3M-*-OIAYBC**

✓

Действительна до 3 июня 2025

Образы VM

Доступные образы виртуальных машин для поведенческого анализа

win10-1803-x64

win7-sp1-x64

astralinux-orel-x64

win7-sp1-x64-ics

redos-murom-x64

astralinux-smolensk-x64

win10-22H2-x64

ubuntu-jammy-x64

Источники

Стандартные

Служба Checkme, веб-интерфейс для проверки файлов, расширенный API, API

Лимит обработки

∞

Электронная почта

Почтовый сервер в режиме фильтрации, почтовый сервер в режиме зеркалирования, почтовый сервер с установленным агентом

5 адресов

1 × 5

Сетевой трафик

ICAP-сервер, PT NAD

500 Мбит/с

1 × 500 Мбит/с

Сетевое хранилище

Общая папка, папка-шлюз

1

Рисунок 1. Страница **Лицензия**

В рабочей области страницы расположены:

- Кнопка **Заменить лицензию** для ввода серийного номера новой лицензии.
- Кнопка **Проверить лицензию** для обновления информации о параметрах текущей лицензии. Рядом с кнопкой также отображается дата последней проверки.

- Номер текущей лицензии и срок ее действия.
- Источники для проверки и лимит их обработки в рамках текущей лицензии.

► Чтобы активировать или заменить лицензию в веб-интерфейсе:

1. В главном меню выберите **Система** → **Лицензия**.
2. Нажмите кнопку **Заменить лицензию**.
3. Введите серийный номер лицензии и нажмите кнопку **Заменить**.

Примечание. Рекомендуется сравнить параметры лицензии, перечисленные на странице, с указанными при заказе лицензии. В случае несоответствия вам нужно обратиться в техническую поддержку Positive Technologies.

9. Настройка средств проверки

Через интерфейс PT Email Security вы можете настраивать средства статического и динамического анализа объектов. В зависимости от средства проверки возможности по настройке различаются. Вы можете:

- Включить или выключить средства проверки Positive Technologies, основные или дополнительные антивирусы, проверку через пользовательские YARA-правила.
- Выбрать способ проверки ссылок, который будет использоваться PT Crawler.
- Настроить отличный от основного прокси-сервер HTTP, который будет использоваться для проверки ссылок через PT Crawler.
- Установить и обновить дополнительные антивирусы.

Кроме того, вы можете настроить параметры поведенческого анализа с помощью консольных команд: отключить или включить проверку цифровой подписи кода приложений Windows и отключить или включить проверку артефактов поведенческого анализа для ОС семейства Linux.

В этом разделе

[Настройка средств проверки Positive Technologies \(см. раздел 9.1\)](#)

[Настройка антивирусов \(см. раздел 9.2\)](#)

[Настройка поведенческого анализа \(см. раздел 9.3\)](#)

[Работа с пользовательскими YARA-правилами \(см. раздел 9.4\)](#)

9.1. Настройка средств проверки Positive Technologies

Для проверки объектов PT Email Security может использовать средства проверки, разработанные специалистами компании Positive Technologies. Для настройки таких средств проверки предназначена страница **Средства проверки** → **Экспертиза РТ**.

Статический анализ**PT ESC**

Positive Technologies Expert Security Center

Версия 5.30.0.135310
Версия базы знаний 5.0.0.438 от 13 янв, 03:35
Проверяются Файлы, dropped файлы, дампы памяти, заголовки писем, AMSI-скрипты

 [Параметры](#)**PT IoC**

Positive Technologies Indicators of Compromise

Версия 5.30.0.135310
Версия базы знаний 1.1.0.843 от 12 янв, 23:37

Обработка ссылок**PT Crawler**

Positive Technologies Crawler

Версия 5.30.0.135310
Способ проверки ссылок Простой

 [Параметры](#)**PT Categorizer**

Positive Technologies Categorizer

Версия 5.30.0.135310
Версия базы знаний 1.0.0.1874 от 13 янв, 07:01

 [Параметры](#)**Поведенческий анализ****PT ML**

Positive Technologies Machine Learning

Версия 5.30.0.135310
Версия базы знаний 4.0.0.33 от 17 дек 2025, 08:23

PT DPI

Positive Technologies Deep Packet Inspection

Версия 12.3.7791
Версия сетевых правил 2.0.0.6163 от 13 янв, 12:11

Защита от угроз в почте**PT Anti-Phishing and Anti-Spam**

Positive Technologies Anti-Phishing and Anti-Spam

Версия 5.30.0.135363
Версия базы знаний 1.0.0.43 от 17 дек 2025, 20:58

 [Параметры](#)Рисунок 2. Страница **Экспертиза PT**

В рабочей области страницы расположены панели с информацией о средствах проверки, разделенные с помощью заголовков на группы:

- **Статический анализ** — средства проверки, использующие методы проверки, относящиеся к статическому анализу:
 - PT ESC — средство статического анализа на основе YARA-правил. По ссылке **Параметры** вы можете выбрать типы проверяемых объектов.
 - PT IoC — средство обнаружения индикаторов компрометации в файлах и ссылках.
- **Обработка ссылок** — средства проверки, предназначенные для работы со ссылками:
 - PT Crawler — средство динамической проверки ссылок. По ссылке **Параметры** вы можете выбрать способ проверки и указать прокси-сервер, который будет использоваться только при проверке ссылок.
 - PT Categorizer — средство категоризации ссылок. По ссылке **Параметры** вы можете указать имена доменов, исключаемых при категоризации ссылок. Ссылкам с такими доменами не будут присваиваться категории.
- **Поведенческий анализ** — средства проверки, использующие методы проверки, относящиеся к поведенческому анализу:
 - PT ML — средство поведенческого анализа на основе технологии машинного обучения.
 - PT DPI — средство поведенческого анализа сетевых пакетов.
- **Защита от угроз в почте** — средства проверки, предназначенные для проверки писем:
 - PT Anti-Phishing and Anti-Spam — средство проверки для выявления признаков фишинга и спама в письмах, а также для проверки найденных в письмах IP-адресов и имен доменов по спискам DNS-блокировок. По ссылке **Параметры** вы можете указать DNS-серверы для разрешения адресов.

Отключение и включение средства проверки Positive Technologies

Примечание. После включения средства проверки начнется обновление его базы знаний, что может занять продолжительное время. Средство проверки начнет работать только после завершения обновления.

- ▶ Чтобы отключить (включить) средство проверки:
 1. В главном меню выберите **Средства проверки** → **Экспертиза PT**.
 2. В панели с информацией о средстве проверки отключите (включите) его.
Статус средства проверки изменится на **Отключен (Включен)**.

Выбор объектов для проверки PT ESC

► Чтобы выбрать объекты для проверки PT ESC:

1. В главном меню выберите **Средства проверки** → **Экспертиза РТ**.
2. В панели с информацией о PT ESC перейдите по ссылке **Параметры**.
3. В блоке параметров **Объекты для проверки** выберите объекты.
4. Нажмите кнопку **Сохранить**.

Добавление прокси-сервера для проверки ссылок

Вы можете указать прокси-сервер, который будет использоваться только при проверке ссылок в объектах от источников.

Внимание! Если прокси-сервер работает в режиме инспекции SSL, для проверки ссылок на нем необходимо отключить использование протоколов SSL и TLS версий 1.0 и 1.1.

► Чтобы добавить прокси-сервер для проверки ссылок:

1. В главном меню выберите **Средства проверки** → **Экспертиза РТ**.
2. В панели с информацией о PT Crawler перейдите по ссылке **Параметры**.
3. В блоке параметров **Прокси-сервер для проверки ссылок** в поле **URL-адрес** введите адрес и порт сервера в формате `http://<Доменное имя или IP-адрес>`.
4. В поля **Логин** и **Пароль** введите учетные данные для аутентификации на сервере.
5. Нажмите кнопку **Сохранить**.

Выбор способа проверки ссылок

Предусмотрены простой и расширенный способы проверки ссылок. В обоих случаях контент по ссылкам скачивается с помощью HTTP/HTTPS-клиента. При расширенном способе проверки, если контент имеет формат HTML, после скачивания формируется полноценная веб-страница: загружаются все связанные ресурсы и выполняются сценарии JavaScript. Это позволяет выявлять динамически создаваемые элементы и потенциально вредоносные сценарии.

► Чтобы выбрать способ проверки ссылок:

1. В главном меню выберите **Средства проверки** → **Экспертиза РТ**.
2. В панели с информацией о PT Crawler перейдите по ссылке **Параметры**.
3. В блоке параметров **Способ проверки ссылок** выберите способ.
4. Нажмите кнопку **Сохранить**.

Настройка категоризации ссылок

При проверке ссылок PT Email Security выполняет категоризацию ссылок и устанавливает для них соответствующие метки. Вы можете указать имена доменов, исключаемых при категоризации ссылок. Ссылкам с такими доменами не будут присваиваться категории.

► Чтобы указать имена доменов, исключаемых при категоризации ссылок:

1. В главном меню выберите **Средства проверки** → **Экспертиза РТ**.
2. В панели с информацией о PT Categorizer перейдите по ссылке **Параметры**.
3. В поле **Исключаемые домены** введите имя домена или поддомена и нажмите клавишу Enter.

Примечание. При вводе имен вы можете использовать звездочку в качестве подстановочного знака.

4. Если требуется указать другие имена, введите их аналогичным образом.
5. Нажмите кнопку **Сохранить**.

Выбор DNS-сервера для разрешения адресов

Разрешение адресов выполняется при их проверке по DNS-спискам блокировок. По умолчанию используется DNS-сервер кластера Kubernetes, развернутого в PT Email Security. Вы можете указать DNS-серверы вашей организации, которые будут использоваться для разрешения адресов.

► Чтобы ввести адрес DNS-сервера:

1. В главном меню выберите **Средства проверки** → **Экспертиза РТ**.
2. В панели с информацией о PT Anti-Phishing and Anti-Spam перейдите по ссылке **Параметры**.
3. Выберите вариант **Указать DNS-серверы**.
4. Введите доменное имя или IP-адрес DNS-сервера.
5. Нажмите кнопку **Сохранить**.

9.2. Настройка антивирусов

Кроме средств проверки, разработанных специалистами Positive Technologies, для проверки объектов в PT Email Security используются антивирусы сторонних разработчиков. Для настройки антивирусов предназначена страница **Средства проверки** → **Антивирусы**.

Основные

Антивирусы и их базы обновляются автоматически с серверов Positive Technologies.

ClamAV

Cisco Talos

Последнее обновление базы 23 июня, 14:34
Версия 0.103.8 от 20 мая, 13:30

PT AV

Positive Technologies

Последнее обновление базы 23 июня, 14:00
Версия 5.3490.0 от 17 июня, 11:21

VBA32

«ВИРУСБЛОКАДА»

Дополнительные

Антивирусы нужно обновлять вручную. Их базы обновляются автоматически с серверов поставщиков.

Kaspersky Web Traffic Security

«Лаборатория Касперского»

Последнее обновление базы 24 июня, 07:43
Версия продукта 6.1.0.4762
Версия ядра 6.1.0.4762
Установлен 24 июня, 09:44
Лицензия  Действительна до 11 сентября

 [Параметры](#)**Доступны к установке**

Антивирусы нужно устанавливать вручную, используя дистрибутив.

Avast Core Security

AVAST Software

 [Установить](#)Рисунок 3. Страница **Антивирусы**

В рабочей области страницы расположены панели с информацией об антивирусах, разделенные с помощью заголовков на группы:

- **Основные** — входят в комплект поставки PT Email Security:
 - ClamAV;
 - PT AV;
 - VBA32.

Базы и лицензии этих антивирусов обновляются автоматически. Вы не можете удалить основные антивирусы, но при необходимости можете их отключить.

- **Дополнительные** — добавлены в PT Email Security после его установки.

Базы дополнительных антивирусов обновляются автоматически с серверов разработчиков или с указанных вами локальных серверов обновлений. Устанавливать новые версии и обновлять лицензии дополнительных антивирусов вам нужно самостоятельно. При необходимости вы можете отключить дополнительные антивирусы или удалить их.

Примечание. При поддержке PT Email Security новой версии дополнительного антивируса в блоке с информацией об этом антивирусе появится оповещение о новой версии. В этом случае вам необходимо самостоятельно обновить антивирус.

В панели каждого дополнительного антивируса расположена ссылка **Параметры** для загрузки файла лицензии и настройки сервера обновлений.

- **Доступны к установке** — антивирусы, которые можно приобрести и добавить в PT Email Security для повышения вероятности обнаружения угроз:

- Avast Core Security 3.0.3;
- Kaspersky Web Traffic Security 6.1.0.4762.

Внимание! В PT Email Security можно установить только указанные версии антивирусов; вы можете скачать их с сайтов разработчиков. Для получения дополнительной информации обратитесь в техническую поддержку Positive Technologies.

В панели каждого доступного для установки антивируса расположена ссылка **Установить** для загрузки файла дистрибутива, файла лицензии и настройки сервера обновлений.

Отключение и включение антивируса

Вы можете отключать проверку объектов отдельными антивирусами. Это может понадобиться, если антивирус показывает множество ложных результатов или требуется временно уменьшить нагрузку на информационную систему организации. Отключенный антивирус можно снова включить в любой момент.

- Чтобы отключить (включить) антивирус:

1. В главном меню выберите **Средства проверки** → **Антивирусы**.
2. В панели с информацией об антивирусе отключите (включите) его.

Статус антивируса изменится на **Отключен (Включен)**.

Установка дополнительного антивируса

Для установки дополнительного антивируса вам понадобятся его дистрибутив и файл лицензии. Вам необходимо самостоятельно приобрести лицензию и установить ее в PT Email Security. Приобрести лицензию вы можете у поставщика антивируса. Лицензия должна быть рассчитана на использование антивируса на двух или более узлах. Требования к количеству пользователей не предъявляются.

Примечание. Если установка одного из поддерживаемых PT Email Security дополнительных антивирусов недоступна, обратитесь в техническую поддержку Positive Technologies.

► Чтобы установить дополнительный антивирус:

1. В главном меню выберите **Средства проверки** → **Антивирусы**.
2. В группе **Доступны к установке** в панели с информацией об антивирусе перейдите по ссылке **Установить**.
3. Перетащите в блок параметров **Загрузить дистрибутив** файл дистрибутива антивируса.
4. Перетащите в блок параметров **Загрузить файл лицензии** файл с лицензией антивируса.
5. Если для скачивания обновлений вы планируете использовать локальный сервер обновлений, включите использование такого сервера и в поле **URL-адрес** введите его адрес в формате <Протокол>://<Доменное имя или IP-адрес>.
6. Если для подключения к локальному серверу обновлений необходимо использовать прокси-сервер, установите флажок **Подключаться через прокси-сервер**.

Примечание. Необходимость использовать прокси-сервер может возникнуть, если сервер обновлений расположен вне закрытой локальной сети организации. В этом случае будет использоваться тот же прокси-сервер, который настроен в PT Email Security для доступа к внешним ресурсам.

7. Нажмите кнопку **Установить**.

По завершении установки в группе **Дополнительные** появится панель с информацией об антивирусе.

Обновление дополнительного антивируса

► Чтобы обновить дополнительный антивирус:

1. В главном меню выберите **Средства проверки** → **Антивирусы**.
2. В панели с информацией об антивирусе перейдите по ссылке **Параметры**.
3. Перетащите в блок параметров **Загрузить дистрибутив** файл дистрибутива антивируса.
4. Нажмите кнопку **Сохранить**.

Замена лицензии дополнительного антивируса

- ▶ Чтобы заменить лицензию дополнительного антивируса:
 1. В главном меню выберите **Средства проверки** → **Антивирусы**.
 2. В панели с информацией об антивирусе перейдите по ссылке **Параметры**.
 3. Перетащите в блок параметров **Лицензия** файл с лицензией антивируса.
 4. Нажмите кнопку **Сохранить**.

Удаление дополнительного антивируса

- ▶ Чтобы удалить дополнительный антивирус:
 1. В главном меню выберите **Средства проверки** → **Антивирусы**.
 2. В панели с информацией об антивирусе перейдите по ссылке **Параметры**.
 3. Нажмите кнопку **Удалить антивирус** и подтвердите удаление.

9.3. Настройка поведенческого анализа

С помощью консольных команд вы можете настраивать некоторые параметры поведенческого анализа файлов.

Проверка цифровой подписи кода приложений Windows

В ходе поведенческого анализа файлов в образах виртуальных машин Windows выполняется проверка цифровой подписи кода приложений Windows (code signing) для файлов форматов DLL, EXE, MSI. Подтверждение цифровой подписи указывает на то, что файл не был изменен и что сертификат удостоверяющего центра не был отозван. Высока вероятность, что такой файл не является вредоносным, но окончательное решение о результате проверки выносится на основании всех используемых методов. Инструкции необходимо выполнять на основном узле.

- ▶ Чтобы отключить проверку цифровой подписи файлов,
выполните команду:

```
sudo ptmsctl system components set -c scan-machine -p check_sample_signature=false
```
- ▶ Чтобы включить проверку цифровой подписи,
выполните команду:

```
sudo ptmsctl system components set -c scan-machine -p check_sample_signature=true
```

9.4. Работа с пользовательскими YARA-правилами

В PT Email Security используется средство проверки объектов по пользовательским YARA-правилам. Вы можете отключать и включать это средство проверки.

Для работы с пользовательскими YARA-правилами предназначена страница **Средства проверки** → **Пользовательские правила**.

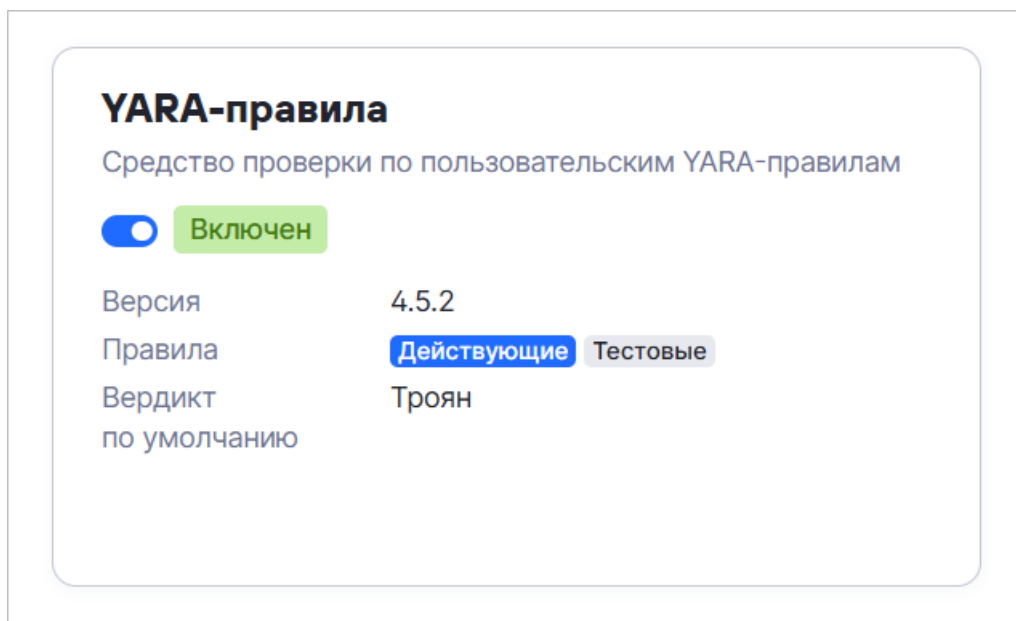


Рисунок 4. Страница **Пользовательские правила**

В рабочей области страницы расположена панель с информацией о средстве проверки по пользовательским YARA-правилам. В панели отображаются:

- Статус средства проверки. При необходимости вы можете отключать и включать средство проверки.
- Версия средства проверки.
- Статус добавленных правил: **Действующие** — результат проверки по таким правилам учитывается при вынесении вердикта; **Тестовые** — результат проверки отображается в карточке объекта, но не влияет на вердикт.

Отключение и включение средства проверки

► Чтобы отключить (включить) средства проверки по YARA-правилам:

1. В главном меню выберите **Средства проверки** → **Пользовательские правила**.
2. В панели **YARA-правила** отключите (включите) средство проверки.

Статус средства проверки изменится на **Отключен** (**Включен**).

10. Настройка основных параметров PT Email Security

Для настройки основных параметров PT Email Security предназначена страница **Основные параметры**. Страница открывается при выборе в главном меню **Система** → **Основные параметры**.

Хранилище

Всего 76 ГБ

Зарезервировано 75,46 ГБ Осталось нераспределенным 0,54 ГБ

● Системные файлы	Зарезервировано	8,46 ГБ
● Образы виртуальных машин	Зарезервировано	48 ГБ
● Файлы заданий	Зарезервировано	15 ГБ
Используется 1,62 ГБ Файлов 1904 / 4 843 257		
Доступно от 3 ГБ до 16.54 ГБ		
● Карантин	Зарезервировано	3 ГБ
Используется 0 ГБ Файлов 13 / 908 110		
Доступно от 3 ГБ до 3.54 ГБ		

Сохранить **Отмена**

Рисунок 5. Страница **Основные параметры**

В рабочей области страницы расположены следующие блоки параметров:

- **Хранилище** — для настройки объема хранилища для файлов заданий.
- **Карантин** — для настройки срока хранения заблокированных писем в карантине.
- **История проверок** — для изменения времени хранения информации о заданиях и проверенных объектах.
- **Отправка сообщений в системный журнал по протоколу syslog** — для настройки отправки событий PT Email Security [во внешние системы в формате сообщений syslog \(см. раздел 14.2\)](#).

- **Отправка данных в PT Threat Analyzer** — для настройки отправки данных об обнаруженных опасных и потенциально опасных объектах в программную платформу PT Threat Analyzer. Вы также можете настроить [отправку найденных в задании файлов с угрозами \(см. раздел 14.7\)](#).
- **Уведомления об угрозах** — для настройки отправки уведомлений об обнаруженных файлах с угрозами по электронной почте.
- **Анонимная проверка** — для предоставления пользователям возможности анонимно проверять файлы и ссылки.
- **Параметры подключения к API** — для ввода дополнительных IP-адресов службы публичного API PT Email Security.

В нижней части страницы расположены кнопки **Сохранить** и **Отменить** для применения или отмены внесенных изменений.

Настройка хранилища для файлов заданий

Файлы всех заданий сохраняются в хранилище. Вы можете указать размер раздела хранилища, который будет зарезервирован для хранения файлов заданий. В этот раздел помещаются файлы, размер которых не превышает 1 ГБ или 1% от размера раздела.

Внимание! Уменьшение размера раздела для файлов заданий может привести к потере сохраненных файлов. Также не рекомендуется часто изменять размер раздела, это может приостановить проверку объектов и привести к задержкам при выполнении заданий.

Файлы заданий удаляются из раздела если: раздел заполнен на 90%; в разделе осталось менее 1 ГБ свободного места; количество файлов в разделе превысило 95% от количества, разрешенного файловой системой. Сперва удаляются самые старые файлы.

► Чтобы изменить размер раздела хранилища для файлов заданий:

1. В главном меню выберите **Система** → **Основные параметры**.
2. В блоке параметров **Хранилище** в строке **Файлы заданий** введите размер раздела в ГБ.
3. Нажмите кнопку **Сохранить**.

Настройка карантина

В карантин помещаются письма с угрозами, заблокированные в результате проверки. Специалист по безопасности может проанализировать содержимое письма в карантине и пропустить его в информационную систему, если признает письмо безопасным. При настройке карантина вы можете:

- Указать размер раздела хранилища, который будет зарезервирован для помещенных в карантин писем. В карантин могут помещаться письма, размер которых не превышает 1 ГБ. Письма удаляются из карантина если: раздел заполнен на 90%; в разделе осталось менее 1

ГБ свободного места; количество писем в разделе превысило 95% от количества, разрешенного файловой системой. Сперва удаляются самые старые письма, при этом помещение новых писем в карантин не ограничивается.

- Указать срок хранения писем в карантине. Письма с истекшим сроком хранения удаляются из карантина.
- Настроить резервный почтовый сервер для пересылки заблокированных писем. Если резервный сервер не настроен, используется почтовый сервер, указанный в параметрах источника.

Примечание. Резервный почтовый сервер всегда используется для источника с типом «Сервер Microsoft Exchange с установленным агентом». Для источника с типом «Почтовый сервер в режиме фильтрации» резервный почтовый сервер используется только если источник отключен или удален.

► Чтобы настроить карантин:

1. В главном меню выберите **Система** → **Основные параметры**.
2. В блоке параметров **Хранилище** в строке **Карантин** введите размер раздела в ГБ.
3. В блоке параметров **Карантин** в поле **Срок хранения в карантине** введите количество дней.
4. Если необходимо использовать резервные почтовые серверы для отправки заблокированных писем, включите их использование и настройте параметры:
 - В раскрывающемся списке **Доверенные сертификаты TLS-шифрования** выберите какой набор доверенных сертификатов будет использоваться для проверки сертификатов почтовых серверов.
 - В блоке параметров **Требования к TLS-шифрованию** укажите для всех почтовых серверов в правиле, требуется ли TLS-шифрование.
 - Если при шифровании требуется проверять сертификат почтового сервера, установите флажок **Проверять сертификат**.
 - В поле **Доменное имя или IP-адрес** введите адрес и порт сервера.
 - Если в вашей организации используется несколько почтовых серверов, в поле **Приоритет** введите число, соответствующее приоритету сервера с указанным адресом.

Примечание. Вы можете указать число от 1 до 65535. Чем меньше число, тем выше приоритет сервера. Письма будут отправляться на активные серверы с наибольшим приоритетом. Если для серверов указан одинаковый приоритет, почтовый трафик балансируется между ними поровну.

- В раскрывающемся списке **Режим запуска TLS-шифрования** выберите режим запуска шифрования для этого сервера.
- Если для доступа к серверу требуется аутентификация, включите использование аутентификации и в раскрывающемся списке **Тип аутентификации** выберите ее тип.

Примечание. При автоматическом выборе типа аутентификации PT Email Security выбирает наиболее безопасный тип из предложенных почтовым сервером.

- Если используется аутентификация, в поля **Логин** и **Пароль** введите учетные данные для доступа к серверу.
- Если в вашей организации используются несколько резервных почтовых серверов, по кнопке **Добавить сервер** добавьте для них блоки параметров и настройте аналогичным образом.

5. Нажмите кнопку **Сохранить**.

Настройка срока хранения заданий

Задания на проверку сохраняются 3 года. Задания с истекшим сроком хранения удаляются блоками, содержащими данные за один календарный месяц. Например, если срок хранения задания истекает в середине месяца, оно будет удалено только по окончании этого месяца.

► Чтобы изменить срок хранения заданий:

1. В главном меню выберите **Система** → **Основные параметры**.
2. В блоке параметров **История проверок** в раскрывающемся списке выберите срок хранения заданий.
3. Нажмите кнопку **Сохранить**.

Настройка почтовых уведомлений об угрозах

Вы можете настроить отправку по электронной почте уведомлений об обнаруженных PT Email Security файлах с угрозами. Для каждого задания уведомления отправляются только при обнаружении первого опасного и первого потенциально опасного файла.

В уведомлении указываются имя файла с угрозой, класс обнаруженного вредоносного ПО, название и тип источника, с которого поступил файл, информация о том, откуда и куда был направлен файл. В теме письма с уведомлением указывается идентификатор задания, в котором обнаружен файл с угрозой, а по кнопке в теле письма вы можете открыть карточку этого задания.

► Чтобы настроить отправку почтовых уведомлений об угрозах:

1. В главном меню выберите **Система** → **Основные параметры**.
2. В блоке параметров **Уведомления об угрозах** включите отправку почтовых уведомлений.
3. В блоке параметров **Отправка уведомлений** выберите, в каких случаях требуется отправлять уведомления:
 - Если только при обнаружении опасных файлов, выберите **Только об опасных файлах**.

- Если при обнаружении опасных и потенциально опасных файлов, выберите **Об опасных и потенциально опасных**.
4. В поле **Эл. адрес отправителя** введите адрес, который будет указан в письме с уведомлением в качестве отправителя.
 5. В поле **Эл. адреса получателей** введите адреса, на которые будут отправляться письма с уведомлениями.
 6. Если требуется изменить язык уведомления, в раскрывающемся списке **Язык уведомлений** выберите нужный язык.
 7. В блоке параметров **SMTP-серверы** настройте параметры доступа к SMTP-серверу для отправки писем с уведомлениями:
 - В поле **Доменное имя или IP-адрес** введите адрес и порт сервера.
 - Если в вашей организации используется несколько почтовых серверов, в поле **Приоритет** введите число, соответствующее приоритету сервера с указанным адресом.

Примечание. Вы можете указать число от 1 до 65535. Чем меньше число, тем выше приоритет сервера. Письма будут отправляться на активные серверы с наибольшим приоритетом. Если для серверов указан одинаковый приоритет, почтовый трафик балансируется между ними поровну.

 - В раскрывающемся списке **Режим запуска TLS-шифрования** выберите режим запуска шифрования для этого сервера.
 - Если для доступа к серверу требуется аутентификация, включите использование аутентификации и в раскрывающемся списке **Тип аутентификации** выберите ее тип.

Примечание. При автоматическом выборе типа аутентификации PT Email Security выбирает наиболее безопасный тип из предложенных почтовым сервером.

 - Если используется аутентификация, в поля **Логин** и **Пароль** введите учетные данные для доступа к серверу.
 - Если в вашей организации используются несколько SMTP-серверов, по кнопке **Добавить сервер** добавьте для них блоки параметров и настройте аналогичным образом.
 8. Нажмите кнопку **Сохранить**.

Включение анонимной проверки объектов

По умолчанию пользователи не могут проверять объекты анонимно (без входа в PT Email Security). Если политика информационной безопасности организации разрешает анонимную проверку, вы можете включить ее.

► Чтобы включить анонимную проверку объектов:

1. В главном меню выберите **Система** → **Основные параметры**.
2. В блоке параметров **Анонимная проверка** включите проверку.
3. Нажмите кнопку **Сохранить**.

Добавление IP-адресов службы публичного API

По умолчанию для подключения к публичному API используется IP-адрес основного узла PT Email Security.

► Чтобы добавить дополнительные адреса службы публичного API PT Email Security:

1. В главном меню выберите **Система** → **Основные параметры**.
2. В блоке параметров **Параметры подключения к API** в поле **IP-адреса службы публичного API** введите дополнительные адреса.
3. Нажмите кнопку **Сохранить**.

Настройка времени отображения письма в очереди MTA

По умолчанию письмо отображается в очереди не менее 28 дней. Вы можете изменить это время. Если обработка продлится дольше, письмо остается в очереди до ее завершения.

► Чтобы изменить времени отображения письма в очереди MTA:

1. В главном меню выберите **Система** → **Параметры очереди обработки писем MTA**.
2. В поле **Время отображения писем в очереди** введите время в днях.
3. Нажмите кнопку **Сохранить**.

11. Работа с токенами доступа

Токен доступа — это уникальная последовательность символов, которая применяется для защиты PT Email Security от несанкционированного доступа через публичный API. Используется при подключении к PT Email Security внешних систем в качестве источников объектов.

Примечание. Доступ к результатам проверки объекта и информации о задании вы можете получить только с тем же токеном доступа, с которым объект был отправлен на проверку.

Вы можете работать с токенами доступа при помощи консольных команд или через веб-интерфейс PT Email Security. Работа с токенами доступа с помощью команд описана в Руководстве разработчика.

Работать с токенами доступа через веб-интерфейс PT Email Security можно на странице **Система → Токены доступа**.

+ Создать токен доступа

↶ Вернуться к фильтру по умолчанию

Дата создания За все время	↓	Кто создал	Название	Связанный источник	Разрешенные действия	Комментарий
27 апр 2024, 13:49		Administrator	token-edr	edr-emakridi	Проверка с параметрами источника	
17 апр 2024, 16:59		Administrator	test		Проверка с передаваемыми параметрами, ...	
22 мар 2024, 15:32		Administrator	maxpatroledr		Проверка с параметрами источника	
14 мар 2024, 13:20		Administrator	maxpatroledrtoken		Проверка с параметрами источника	
6 мар 2024, 09:59		Administrator	oc-token	oc-entryptpoint	Проверка с параметрами источника	
6 мар 2024, 09:34		Administrator	oc-key		Проверка с передаваемыми параметрами	
21 фев 2024, 15:06		Administrator	api-entry-point-token	api-entry-point	Проверка с параметрами источника	
26 янв 2024, 05:06		Administrator	ptcs2avscanner	ptcs-av-scanner	Проверка с передаваемыми параметрами, ...	for PT CS

Всего 70

1

2

<

>

Рисунок 6. Страница **Токены доступа**

В рабочей области страницы расположены:

- Кнопка **Создать токен доступа**, при нажатии которой открывается окно для создания нового токена доступа.
- Таблица с информацией по всем созданным токенам доступа. При наведении курсора на строку таблицы отображаются значки:
 -  — для изменения комментария к токenu.
 -  — для отзыва токена доступа. Если токен привязан к источнику, то после его отзыва источник перестанет работать.

Ниже приведены инструкции по работе с токенами доступа.

Создание токена доступа

► Чтобы создать токен доступа:

1. В главном меню выберите **Система** → **Токены доступа**.
2. Нажмите кнопку **Создать токен доступа**.
3. Введите название токена доступа. Оно будет отображаться на странице **Токены доступа**.
4. Выберите разрешенные действия, которые будут доступны при использовании токена.
5. Нажмите кнопку **Создать**.

Созданный токен доступа отобразится в окне **Токен доступа создан**.

6. Нажмите кнопку **Скопировать в буфер обмена и закрыть**, чтобы скопировать токен.

Внимание! После закрытия этого окна токен будет недоступен для просмотра и копирования.

Отзыв токена доступа

Вы можете отозвать токен доступа. Если токен доступа используется источником, то он перестанет работать после отзыва токена. Если токен доступа используется сторонней системой, то ее работа также может быть нарушена.

► Чтобы отозвать токен доступа:

1. В главном меню выберите **Система** → **Токены доступа**.
2. В строке с токеном доступа нажмите .
3. Нажмите кнопку **Все равно отозвать**.

12. Работа с источниками

Источник для проверки (источник) — интерфейс в информационной системе организации, с которого в PT Email Security поступают объекты на проверку.

Объекты могут поступать на проверку от встроенных источников, которые не требуется добавлять в PT Email Security, и от подключаемых внешних источников, которые необходимо добавлять в PT Email Security в соответствии с их типами.

Встроенные источники

В PT Email Security предусмотрены следующие встроенные источники:

- Веб-интерфейс — вы можете анонимно или после входа в PT Email Security отправить объекты на проверку через веб-интерфейс. Поддерживается проверка объектов размером до 1 ГБ.
- Хранилище файлов — после настройки параметров повторной проверки PT Email Security регулярно проверяет файлы в хранилище.
- API с передаваемыми параметрами проверки — внешняя система может передавать объекты на проверку через службу публичного API PT Email Security. Проверка выполняется с параметрами, переданными в запросе. Поддерживается проверка объектов размером до 1 ГБ.

Подключаемые источники

Источником объектов для PT Email Security может служить внешняя система, например почтовый сервер, межсетевой экран или папки на сетевом диске. При подключении внешней системы, как правило, требуется настроить саму систему для работы с PT Email Security и добавить эту систему в PT Email Security в качестве источника. Для подключения различных типов внешних систем предусмотрены следующие типы источников:

- Служба Checkme — служба для проверки объектов по электронной почте, обеспечивает взаимодействие PT Email Security с почтовым сервером вашей организации. После настройки этого источника для проверки объекта достаточно отправить его письмом на специальный адрес электронной почты. PT Email Security проверит само письмо, ссылки в тексте письма и вложенные в него файлы. Результат проверки отправляется в ответном письме. Поддерживается проверка писем размером до 1 ГБ.
- Общая папка — папка с настроенным общим доступом, все файлы которой проверяются PT Email Security. После проверки все файлы остаются в той же папке. Поддерживается проверка файлов размером до 5 ГБ.
- Папка-шлюз — папка с настроенным общим доступом, все файлы которой проверяются PT Email Security. По результатам проверки объекты из папки-шлюза переносятся в папку для безопасных объектов или папку карантина. Поддерживается проверка файлов размером до 5 ГБ.

- ICAP-сервер — позволяет принимать на проверку объекты по протоколу ICAP. Для этого в PT Email Security настраивается ICAP-сервер, а внешняя система выступает в качестве ICAP-клиента. Поддерживается проверка объектов размером до 1 ГБ.
- Почтовый шлюз безопасности — позволяет получать письма от SMTP-сервера, развернутого на внешнем узле. Такой сервер принимает письма от SMTP-клиентов и работает в качестве почтового шлюза.
- Сервер Microsoft Exchange с установленным агентом — позволяет принимать почтовый трафик сервера Microsoft Exchange, перенаправляемый с помощью почтового агента PT Email Security. Почтовый агент устанавливается на сервер Microsoft Exchange, перехватывает все проходящие через сервер письма и отправляет их на проверку в PT Email Security, после чего возвращает проверенные письма обратно для доставки адресатам. Поддерживается проверка писем размером до 1 ГБ.
- Почтовый сервер в режиме фильтрации — позволяет принимать от почтового сервера, работающего в режиме фильтрации, письма для проверки в PT Email Security. Поддерживается проверка писем размером до 1 ГБ.

Режим фильтрации — режим работы почтового сервера, при котором PT Email Security может фильтровать почтовый трафик сервера. В зависимости от выбранного режима проверки PT Email Security либо сразу возвращает почтовому серверу отправленное на проверку письмо (пассивный режим), либо блокирует его до окончания проверки (блокирующий режим).

- Почтовый сервер в режиме фильтрации (MTA) — позволяет то же что и почтовый сервер в режиме фильтрации, но для работы с письмами используется встроенный в PT Email Security почтовый транспортный агент. Поддерживается проверка писем размером до 1 ГБ.
- Почтовый сервер в режиме зеркалирования — позволяет принимать от почтового сервера, работающего в режиме зеркалирования, скрытые копии писем для проверки в PT Email Security. Поддерживается проверка писем размером до 1 ГБ.

Режим зеркалирования — режим работы почтового сервера, при котором PT Email Security не влияет на почтовый трафик сервера. На проверку в PT Email Security отправляются копии писем.

- PT NAD — позволяет настроить интеграцию с PT NAD. После интеграции извлеченные из сетевого трафика файлы отправляются на проверку в PT Email Security. Поддерживается проверка файлов размером до 1 ГБ.
- MaxPatrol EDR — позволяет настроить интеграцию с MaxPatrol EDR. После интеграции извлеченные файлы конечных устройств отправляются на проверку в PT Email Security. Поддерживается проверка файлов размером до 1 ГБ.
- API с выбранными параметрами проверки — позволяет настроить интеграцию с внешними системами через сервис публичного API PT Email Security. Поддерживается проверка объектов размером до 1 ГБ.

Параметры проверки объектов, поступающих от источника, настраиваются индивидуально для каждого источника после его добавления в PT Email Security. Параметры проверки могут отличаться для источников разных типов.

Режимы проверки объектов, поступающих от источников

В зависимости от способа обработки объектов, поступающих на проверку в PT Email Security, предусмотрены следующие режимы проверки:

- Режим ожидания — режим проверки, при котором на проверку от источников в PT Email Security поступают копии объектов, а их распространение контролирует пользователь или сторонняя система.
- Пассивный режим — режим проверки, при котором поступившие на проверку объекты сразу пропускаются PT Email Security в информационную систему.
- Блокирующий режим — режим проверки, при котором поступившие на проверку объекты блокируются PT Email Security до окончания проверки. В зависимости от вынесенного вердикта объект пропускается в информационную систему или удаляется (или помещается в карантин).

Примечание. Использование блокирующего режима может быть ограничено лицензией.

Режимы проверки для каждого типа источника указаны в таблице. Для источников, поддерживающих несколько режимов проверки, выбор режима зависит от политики информационной безопасности вашей организации. Вы можете настроить режим проверки объектов для таких источников в параметрах проверки. Для источников с типом «ICAP-сервер» режим проверки настраивается в параметрах ICAP-клиента.

Таблица 3. Режимы проверки объектов, поступающих от источников

Тип источника	Режим ожидания	Пассивный режим	Блокирующий режим
Веб-интерфейс	Да	—	—
Хранилище файлов	Да	—	—
Служба Checkme	Да	—	—
Общая папка	—	Да	—
Папка-шлюз	—	Да	Да
ICAP-сервер	Да	Да	Да
Почтовый шлюз безопасности	—	Да	Да
Сервер Microsoft Exchange с установленным агентом	—	Да	Да
Почтовый сервер в режиме фильтрации	—	Да	Да
Почтовый сервер в режиме фильтрации (MTA)	—	Да	Да
Почтовый сервер в режиме зеркалирования	—	Да	—

Тип источника	Режим ожидания	Пассивный режим	Блокирующий режим
PT NAD	—	Да	—
MaxPatrol EDR	Да	—	—
API с выбранными параметрами проверки	Да	—	—
API с передаваемыми параметрами проверки	Да	—	—

В этом разделе

[Настройка источников \(см. раздел 12.1\)](#)

[Настройка правил маршрутизации проверенных писем \(см. раздел 12.2\)](#)

[Отключение автоматической смены режимов проверки \(см. раздел 12.3\)](#)

12.1. Настройка источников

PT Email Security может проверять объекты, поступающие от пользователей или из внешних систем, подключенных в качестве источников объектов. Для работы с источниками предназначена страница **Источники**. Страница открывается при выборе в главном меню раздела **Источники**. Вы можете добавлять и удалять источники, изменять их параметры, временно отключать и включать.

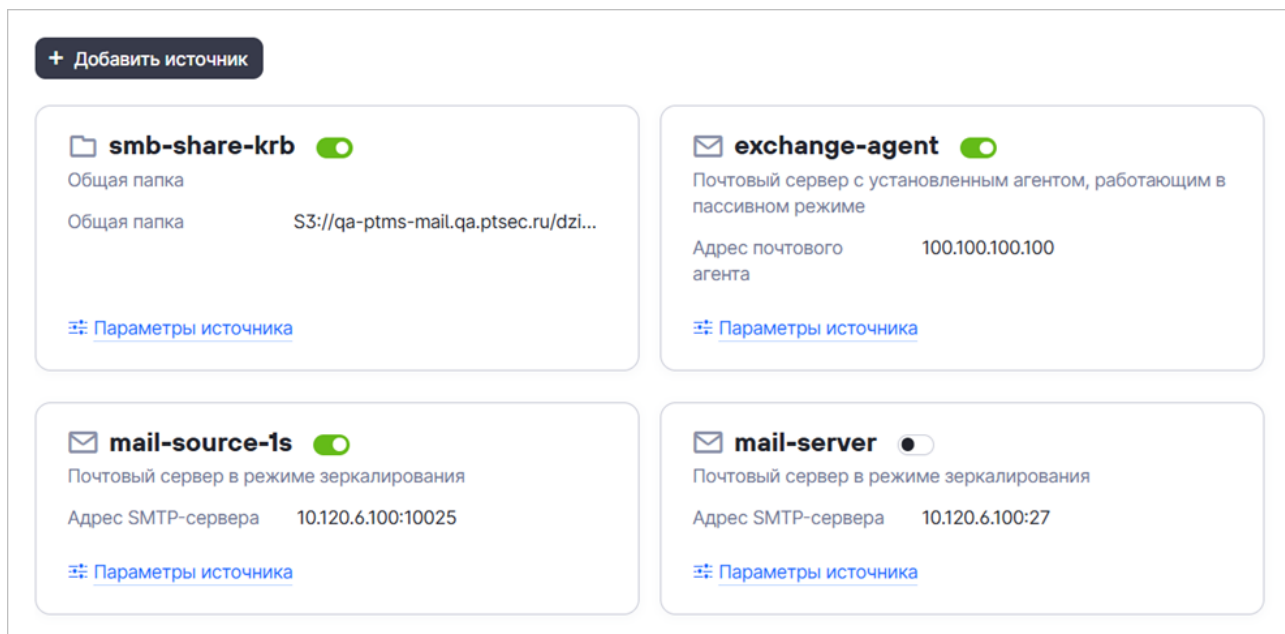


Рисунок 7. Страница **Источники**

Вверху страницы расположена кнопка **Добавить источник** для добавления нового источника для проверки.

В рабочей области страницы расположены панели с информацией о добавленных источниках. При необходимости вы можете отключать источники. В каждой панели расположена ссылка **Параметры источника** для настройки параметров.

Добавление источника

Внимание! Количество подов на любом узле PT Email Security не должно превышать 150. При добавлении источника в PT Email Security на основном узле для его работы создаются два пода. Отслеживать текущее количество созданных подов вы можете на странице **Система** → **Конфигурация** → **Узлы**. Если требуется увеличить максимальное количество подов на узле, обратитесь в техническую поддержку Positive Technologies.

► Чтобы добавить источник в PT Email Security:

1. В главном меню выберите **Источники**.
2. Нажмите кнопку **Добавить источник**.
3. В поле **Название** введите название источника, которое будет указано в свойствах полученных от него объектов.

Название должно содержать не менее пяти символов и быть уникальным среди названий всех источников. Название может содержать только строчные буквы латинского алфавита, цифры, дефис и при этом начинаться и заканчиваться только буквами.

4. В раскрывающемся списке **Тип** выберите тип источника.
5. Укажите параметры подключения источника в зависимости от его типа.
6. Нажмите кнопку **Добавить источник**.

Изменение параметров источника

► Чтобы изменить параметры источника:

1. В главном меню выберите **Источники**.
2. В панели с информацией об источнике перейдите по ссылке **Параметры источника**.
3. Измените параметры источника.

Примечание. Вы можете изменить любые параметры источника, кроме его названия и типа.

4. Нажмите кнопку **Сохранить**.

Отключение и включение источника

► Чтобы отключить (включить) источник:

1. В главном меню выберите **Источники**.
2. В панели с информацией об источнике отключите (включите) его.

Удаление источника

► Чтобы удалить источник:

1. В главном меню выберите **Источники**.
2. В панели с информацией об источнике перейдите по ссылке **Параметры источника**.
3. Нажмите  и подтвердите удаление.

12.2. Настройка правил маршрутизации проверенных писем

Если в вашей организации используются несколько почтовых серверов, для источника с типом «Почтовый сервер в режиме фильтрации» вы можете настроить правила маршрутизации проверенных писем. В зависимости от домена, указанного в электронном адресе получателя письма, PT Email Security может отправлять письма и уведомления о результатах проверки на определенные почтовые серверы. В правиле маршрутизации вы можете выбрать один из способов маршрутизации: по MX-записям, имеющимся в DNS для почтового домена, или на указанные почтовые серверы (согласно их приоритету).

Правила маршрутизации проверенных писем настраиваются отдельно для каждого источника. Вы можете добавлять, изменять и удалять правила. Добавленное ранее правило вы можете скопировать для того же или другого источника.

Добавление правила маршрутизации

► Чтобы добавить правило маршрутизации:

1. В главном меню выберите **Источники**.
2. В панели с информацией об источнике перейдите по ссылке **Параметры источника**.
3. В блоке параметров **Правила маршрутизации почтового трафика** нажмите кнопку **Добавить**.
4. В поле **Домен электронной почты получателя** введите доменную часть адреса электронной почты получателей, для которых необходимо настроить правило.

С помощью звездочки вы можете задать маску для доменной части адреса получателей писем, если доменная часть содержит поддомены третьего уровня или выше. Например, правило с маской *.example.com будет применяться и для адресов с доменной частью example.com, sub_1.example.com, sub_2.example.com, и для адресов с доменной частью, содержащей поддомены более высоких уровней.

Примечание. Если доменная часть адреса получателя соответствует нескольким правилам маршрутизации, будет использовано то правило, в котором указан наиболее точный адрес. При этом более высокий приоритет имеют правила, в которых не используются маски.

5. В блоке параметров **Требования к TLS-шифрованию** укажите для всех почтовых серверов в правиле, требуется ли TLS-шифрование.
6. Если при шифровании требуется проверять сертификат почтового сервера, установите флажок **Проверять сертификат**.
7. Если необходимо перенаправлять письма согласно MX-записям, выберите способ маршрутизации **По MX-записям**.

Внимание! Письмо не будет отправлено, если в DNS отсутствует подходящая MX- или A-запись для указанного домена.

8. Если необходимо перенаправлять письма на определенный почтовый сервер, выберите способ маршрутизации **По адресам почтовых серверов** и укажите параметры сервера:
 - В поле **Доменное имя или IP-адрес** введите адрес и порт сервера.
 - Если в вашей организации используется несколько почтовых серверов, в поле **Приоритет** введите число, соответствующее приоритету сервера с указанным адресом.

Примечание. Вы можете указать число от 1 до 65535. Чем меньше число, тем выше приоритет сервера. Письма будут отправляться на активные серверы с наибольшим приоритетом. Если для серверов указан одинаковый приоритет, почтовый трафик балансируется между ними поровну.

- В раскрывающемся списке **Режим запуска TLS-шифрования** выберите режим запуска шифрования для этого сервера.
- Если для доступа к серверу требуется аутентификация, включите использование аутентификации и в раскрывающемся списке **Тип аутентификации** выберите ее тип.

Примечание. При автоматическом выборе типа аутентификации PT Email Security выбирает наиболее безопасный тип из предложенных почтовым сервером.

- Если используется аутентификация, в поля **Логин** и **Пароль** введите учетные данные для доступа к серверу.
- Если в вашей организации используется несколько почтовых серверов, по кнопке **Добавить сервер** добавьте для них блоки параметров и настройте аналогичным образом.

9. Нажмите кнопку **Добавить**.

10. Нажмите кнопку **Сохранить**.

Правило маршрутизации добавлено.

Копирование правила маршрутизации

► Чтобы скопировать правило маршрутизации:

1. В главном меню выберите **Источники**.

2. В панели с информацией об источнике нажмите кнопку **Параметры проверки**.

3. В блоке параметров **Правила маршрутизации почтового трафика** в строке правила, которое вы хотите скопировать, нажмите .

4. Нажмите кнопку **Вставить правило**.

Откроется окно **Добавление правила**.

5. Нажмите кнопку **Добавить**.

6. Нажмите кнопку **Сохранить**.

Правило маршрутизации скопировано.

Изменение правила маршрутизации

► Чтобы изменить правило маршрутизации:

1. В главном меню выберите **Источники**.

2. В панели с информацией об источнике нажмите кнопку **Параметры проверки**.

3. В блоке параметров **Правила маршрутизации почтового трафика** в строке правила, которое вы хотите изменить, нажмите .

Откроется окно **Изменение правила**.

4. Измените правило.

5. Нажмите кнопку **Изменить**.

6. Нажмите кнопку **Сохранить**.

Правило маршрутизации изменено.

Удаление правила маршрутизации

► Чтобы удалить правило маршрутизации:

1. В главном меню выберите **Источники**.
2. В панели с информацией об источнике нажмите кнопку **Параметры проверки**.
3. В блоке параметров **Правила маршрутизации почтового трафика** в строке правила, которое вы хотите удалить, нажмите  и подтвердите удаление.
4. Нажмите кнопку **Сохранить**.

Правило маршрутизации удалено.

12.3. Отключение автоматической смены режимов проверки

Для источников с типами «Почтовый сервер в режиме фильтрации» и «Сервер Microsoft Exchange с установленным агентом» при большом количестве поступающих на проверку писем блокирующий режим проверки может автоматически меняться на пассивный. Это позволяет вовремя доставлять письма адресатам, но может привести к тому, что письма с угрозами попадут в информационную систему организации. После снижения нагрузки возвращается блокирующий режим проверки. Вы можете отключить для выбранных источников автоматическую смену режимов проверки. Инструкции необходимо выполнять на основном узле.

Внимание! После отключения автоматической смены режимов проверки для источника в случае нештатного прекращения проверки писем в PT Email Security письма от этого источника не будут доставляться адресатам.

► Чтобы отключить автоматическую смену режимов проверки для источника,

выполните команду:

```
sudo ptmsctl system components config patch --component <Название источника> --toml "[statistic]
enable_downgrade = false
"
```

► Чтобы включить автоматическую смену режимов проверки для источника,

выполните команду:

```
sudo ptmsctl system components config patch --component <Название источника> --toml "[statistic]
enable_downgrade = true
"
```

13. Подключение источников

В разделе описаны возможности подключения к PT Email Security источников объектов для проверки.

Внимание! Количество подов на любом узле PT Email Security не должно превышать 150. При добавлении источника в PT Email Security на основном узле для его работы создаются два пода. Отслеживать текущее количество созданных подов вы можете на странице **Система** → **Конфигурация** → **Узлы**. Если требуется увеличить максимальное количество подов на узле, обратитесь в техническую поддержку Positive Technologies.

Примечание. Если подключение источника какого-либо типа недоступно, обратитесь в техническую поддержку Positive Technologies.

В этом разделе

[Служба Checkme \(см. раздел 13.1\)](#)

[Общая папка \(см. раздел 13.2\)](#)

[Папка-шлюз \(см. раздел 13.3\)](#)

[S3-хранилище \(см. раздел 13.4\)](#)

[Внешняя система как ICAP-клиент \(см. раздел 13.5\)](#)

[Внешняя система через API \(см. раздел 13.6\)](#)

[Почтовый шлюз безопасности \(см. раздел 13.7\)](#)

[«Код безопасности», «Континент» 4.1 \(см. раздел 13.8\)](#)

[Exim 4 в режиме фильтрации \(см. раздел 13.9\)](#)

[Exim 4 в режиме зеркалирования \(см. раздел 13.10\)](#)

[Microsoft Exchange 2010–2019 с установленным почтовым агентом \(см. раздел 13.11\)](#)

[Microsoft Exchange 2010–2019 в режиме зеркалирования \(см. раздел 13.12\)](#)

[Postfix 3.2 в режиме фильтрации \(см. раздел 13.13\)](#)

[Postfix 3.2 в режиме зеркалирования \(см. раздел 13.14\)](#)

[PT Threat Analyzer 2.10 и выше \(см. раздел 13.15\)](#)

[Squid 3 и выше \(см. раздел 13.16\)](#)

[UserGate NGFW 6, 7.1, 7.4 \(см. раздел 13.17\)](#)

13.1. Служба Checkme

PT Email Security может проверять письма и вложенные в них объекты, отправленные сотрудниками вашей организации на специальный электронный адрес. Результат проверки отправляется сотруднику в ответном письме. Служба Checkme обеспечивает взаимодействие PT Email Security с почтовым сервером вашей организации.

Внимание! Если в вашей информационной системе используется межсетевой экран или другие средства контроля сетевого трафика, требуется настроить в них правила, разрешающие передачу трафика через порты TCP 143, 587 или TCP 465, 993 (при подключении по SSL) от основного узла PT Email Security к почтовому серверу вашей организации.

Для создания и настройки службы Checkme необходимо:

- На почтовом сервере вашей организации создать электронный адрес для службы Checkme, например `checkme@example.com`.
- В PT Email Security добавить источник с типом **Служба Checkme** и указать для него параметры подключения к почтовому серверу вашей организации.

Добавление источника в PT Email Security

► Чтобы добавить источник в PT Email Security:

1. В главном меню выберите **Источники**.
2. Нажмите кнопку **Добавить источник**.
3. В поле **Название** введите название источника, которое будет указано в свойствах полученных от него объектов.

Название должно содержать не менее пяти символов и быть уникальным среди названий всех источников. Название может содержать только строчные буквы латинского алфавита, цифры, дефис и при этом начинаться и заканчиваться только буквами.

4. В раскрывающемся списке **Тип** выберите **Служба Checkme**.
5. В блоке **Параметры подключения** настройте параметры IMAP-сервера для приема писем с вложениями для проверки:
 - В поле **Доменное имя или IP-адрес IMAP-сервера** введите адрес и порт сервера.
 - Если соединение с сервером устанавливается по протоколу SSL, установите флажок **Подключаться по SSL**.
 - В раскрывающемся списке **Тип аутентификации IMAP** выберите тип аутентификации при подключении к серверу.

Примечание. При автоматическом выборе типа аутентификации PT Email Security выбирает наиболее безопасный тип из предложенных почтовым сервером.

- В полях **Логин** и **Пароль** введите учетные данные для подключения к серверу.
- 6. Если требуется, в блоке **Отправлять результат проверки в ответном письме** включите отправку писем с результатами проверки и настройте параметры SMTP-сервера для их отправки:
 - В поле **Доменное имя или IP-адрес SMTP-сервера** введите адрес и порт сервера.
 - В раскрывающемся списке **Режим запуска TLS-шифрования** выберите режим запуска шифрования для этого сервера.
 - В раскрывающемся списке **Тип аутентификации IMAP** выберите тип аутентификации при подключении к серверу.
 - В полях **Логин** и **Пароль** введите учетные данные для подключения к серверу.
- 7. В поле **Эл. адрес службы Checkme** введите адрес, на который будут отправлять письма с вложениями для проверки, например `checkme@example.com`.
- 8. Нажмите кнопку **Добавить источник**.

Источник добавлен в PT Email Security.

13.2. Общая папка

Если для обмена файлами сотрудники вашей организации используют общую папку, с помощью PT Email Security вы можете организовать проверку файлов в этой папке. Проверяются все файлы в общей папке и вложенных в нее папках. Для доступа к папке PT Email Security использует протоколы SMB версий 2 и 3, и NFS версии 3.

Внимание! Если в вашей информационной системе используется межсетевой экран или другие средства контроля сетевого трафика, требуется настроить в них правила, разрешающие передачу трафика через порты TCP 139, 445 (SMB) или TCP 111, 2049 (NFS) от основного узла PT Email Security к узлу с общей папкой.

Для подключения общей папки необходимо:

- Создать папку и настроить общий доступ пользователей к этой папке.
- Предоставить PT Email Security право на чтение файлов в созданной папке и всех вложенных в нее папках.
- Добавить в PT Email Security источник с типом **Общая папка**.

Алгоритм работы с общей папкой

Сразу после добавления источника PT Email Security проверяет общую папку на наличие в ней объектов, удовлетворяющих условиям:

- Новый объект, который никогда не проверялся.
- Задание на проверку объекта завершилось с ошибкой более 1 часа назад.
- Задание на проверку объекта завершилось успешно более 4 недель назад и хеш-сумма объекта за это время изменилась.

Если объект в папке удовлетворяет хотя бы одному из условий выше, PT Email Security отслеживает его в течение 2 минут. По истечении этого времени:

- Если объект был изменен — отсчет времени начинается заново.
- Если не был изменен — создается задание на проверку.

Примечание. Одновременно PT Email Security может проверять не более 15 объектов из общей папки.

Повторная проверка общей папки выполняется через 5 минут после завершения предыдущей.

Добавление источника в PT Email Security

► Чтобы добавить источник в PT Email Security:

1. В главном меню выберите **Источники**.
2. Нажмите кнопку **Добавить источник**.
3. В поле **Название** введите название источника, которое будет указано в свойствах полученных от него объектов.

Название должно содержать не менее пяти символов и быть уникальным среди названий всех источников. Название может содержать только строчные буквы латинского алфавита, цифры, дефис и при этом начинаться и заканчиваться только буквами.

4. В раскрывающемся списке **Тип** выберите **Общая папка**.
5. В полях блока **Доменное имя или IP-адрес узла с папкой** укажите параметры подключения к узлу с общей папкой:
 - Выберите протокол подключения **NFS** или **SMB**.
 - Введите доменное имя или IP-адрес узла.
 - Если для подключения используется нестандартный порт, укажите его.
6. Если вы выбрали протокол SMB, укажите параметры аутентификации:
 - В раскрывающемся списке **Тип аутентификации** выберите тип аутентификации.
 - Если вы выбрали **Kerberos**, в поле **IP-адрес контроллера домена** введите адрес.

- В полях **Логин** и **Пароль** введите учетные данные для доступа к папке.

Если вы выбрали тип аутентификации Kerberos, логин необходимо указывать вместе с именем домена в формате <Имя домена>\<Логин>, например yourdomain\ivanov. Если вы выбрали NTLM, вы также можете указать имя домена в этом формате при необходимости.

7. В поле **Путь к папке** введите путь к общей папке.

В качестве разделителя каталогов используйте косую черту /.

8. Нажмите кнопку **Добавить источник**.

Источник добавлен в PT Email Security.

13.3. Папка-шлюз

Если для обмена файлами сотрудники вашей организации используют общую папку, с помощью PT Email Security вы можете настроить папку-шлюз. Проверяются все файлы в папке-шлюзе и вложенных в нее папках. По результатам проверки файлы из папки-шлюза переносятся в папку для безопасных объектов или папку карантина, при необходимости создаются вложенные папки. Для доступа к папкам PT Email Security использует протоколы SMB версий 2, 3 и NFS версии 3.

Внимание! Если в вашей информационной системе используется межсетевой экран или другие средства контроля сетевого трафика, требуется настроить в них правила, разрешающие передачу трафика через порты TCP 139, 445 (SMB) или TCP 111, 2049 (NFS) от основного узла PT Email Security к узлу с папкой-шлюзом.

Для подключения папки-шлюза необходимо:

- Создать три папки и настроить общий доступ пользователей к этим папкам: папку-шлюз, папку для безопасных объектов и папку карантина. Папки могут располагаться на одном или на разных узлах.

Внимание! Папки не должны быть вложены друг в друга.

- Предоставить PT Email Security права на чтение, запись и удаление файлов в созданных папках и всех вложенных в них папках.
- Добавить в PT Email Security источник с типом **Папка-шлюз**.

Алгоритм работы с папкой-шлюзом

Сразу после добавления источника PT Email Security проверяет папку-шлюз на наличие в ней новых объектов или объектов, при проверке которых произошла ошибка.

Если в папке есть такой объект, то PT Email Security отслеживает его в течение 2 минут. По истечении этого времени:

- Если объект был изменен — отсчет времени начинается заново.
- Если не был изменен — создается задание на проверку.

Примечание. Одновременно PT Email Security может проверять не более 30 объектов из папки-шлюза.

После завершения задания на проверку PT Email Security выполняет с объектом одно из действий:

- Если угроз не обнаружено, переносит объект в папку для безопасных объектов.
- Если объект представляет угрозу, переносит его в папку карантина.
- Если задание завершилось с ошибкой, оставляет объект в папке-шлюзе.

Повторная проверка папки-шлюза выполняется через 10 секунд после завершения предыдущей.

Добавление источника в PT Email Security

► Чтобы добавить источник в PT Email Security:

1. В главном меню выберите **Источники**.
2. Нажмите кнопку **Добавить источник**.
3. В поле **Название** введите название источника, которое будет указано в свойствах полученных от него объектов.

Название должно содержать не менее пяти символов и быть уникальным среди названий всех источников. Название может содержать только строчные буквы латинского алфавита, цифры, дефис и при этом начинаться и заканчиваться только буквами.
4. В раскрывающемся списке **Тип** выберите **Папка-шлюз**.
5. В блоке параметров **Папка-шлюз** в полях блока **Доменное имя или IP-адрес узла с папкой** укажите параметры подключения к узлу с папкой-шлюзом:
 - Выберите протокол подключения **NFS** или **SMB**.
 - Введите доменное имя или IP-адрес узла.
 - Если для подключения используется нестандартный порт, укажите его.
6. Если вы выбрали протокол SMB, укажите параметры аутентификации:
 - В раскрывающемся списке **Тип аутентификации** выберите тип аутентификации.
 - Если вы выбрали **Kerberos**, в поле **IP-адрес контроллера домена** введите адрес.
 - В полях **Логин** и **Пароль** введите учетные данные для доступа к папке.

Если вы выбрали тип аутентификации Kerberos, логин необходимо указывать вместе с именем домена в формате <Имя домена>\<Логин>, например yourdomain\ivanov. Если вы выбрали NTLM, вы также можете указать имя домена в этом формате при необходимости.
7. В поле **Путь к папке** введите путь к папке-шлюзу на узле.

В качестве разделителя каталогов используйте косую черту /.

8. В блоке параметров **Папка для безопасных файлов** в полях блока **Доменное имя или IP-адрес узла с папкой** укажите параметры подключения к узлу с папкой для безопасных объектов:
 - Если папка расположена на том же узле, что и папка-шлюз, установите флажок **Такие же параметры, как у сервера папки-шлюза**.
 - Если папка расположена на другом узле, укажите параметры подключения к этому узлу.
9. В поле **Путь к папке** введите путь к папке на узле.
10. В блоке параметров **Папка карантина** в полях блока **Доменное имя или IP-адрес узла с папкой** укажите параметры подключения к узлу с папкой для объектов, представляющих угрозу:
 - Если папка расположена на том же узле, что и папка-шлюз, установите флажок **Такие же параметры, как у сервера папки-шлюза**.
 - Если папка расположена на другом узле, укажите параметры подключения к этому узлу.
11. В поле **Путь к папке** введите путь к папке на узле.
12. Нажмите кнопку **Добавить источник**.

Источник добавлен в PT Email Security.

13.4. S3-хранилище

Если для хранения файлов, писем и других объектов в вашей организации используется S3-хранилище, с помощью PT Email Security вы можете организовать проверку объектов в таком хранилище.

Внимание! Если провайдер S3-хранилища тарифицирует трафик или количество запросов, проверка объектов в PT Email Security может привести к дополнительным расходам.

Внимание! Если в вашей информационной системе используется межсетевой экран или другие средства контроля сетевого трафика, требуется настроить в них правила, разрешающие передачу трафика через порты TCP 80, 443 от узла источника к основному узлу PT Email Security.

Порядок подключения S3-хранилища зависит от провайдера. Как правило, для настройки доступа к хранилищу на сайте провайдера вам необходимо:

- Создать бакет (каталог верхнего уровня) для проверяемых объектов и указать для него название и регион, если предусмотрено провайдером.
- Создать сервисный аккаунт и предоставить ему право на чтение объектов бакета.
- Создать для сервисного аккаунта статический ключ доступа.

Примечание. Инструкции по настройке доступа к S3-хранилищу вы можете найти на сайте провайдера.

Для подключения S3-хранилища необходимо в PT Email Security добавить источник с типом **Общая папка** и протоколом подключения **S3**.

Алгоритм работы с S3-хранилищем

Сразу после добавления источника PT Email Security проверяет хранилище на наличие объектов, удовлетворяющих условиям:

- Новый объект, который никогда не проверялся.
- Задание на проверку объекта завершилось с ошибкой более 1 часа назад.
- Задание на проверку объекта завершилось успешно более 4 недель назад и хеш-сумма объекта за это время изменилась.

Если объект в хранилище удовлетворяет хотя бы одному из условий выше, PT Email Security отслеживает его в течение 2 минут. По истечении этого времени:

- Если объект был изменен — отсчет времени начинается заново.
- Если не был изменен — создается задание на проверку.

Примечание. Одновременно PT Email Security может проверять не более 15 объектов из хранилища.

Повторная проверка хранилища выполняется через 5 минут после завершения предыдущей.

Добавление источника в PT Email Security

► Чтобы добавить источник в PT Email Security:

1. В главном меню выберите **Источники**.
2. Нажмите кнопку **Добавить источник**.
3. В поле **Название** введите название источника, которое будет указано в свойствах полученных от него объектов.

Название должно содержать не менее пяти символов и быть уникальным среди названий всех источников. Название может содержать только строчные буквы латинского алфавита, цифры, дефис и при этом начинаться и заканчиваться только буквами.

4. В раскрывающемся списке **Тип** выберите **Общая папка**.
5. В полях блока **Доменное имя или IP-адрес узла с папкой** укажите параметры подключения к S3-хранилищу:
 - Выберите протокол подключения **S3**.
 - Введите доменное имя или IP-адрес провайдера хранилища.
 - Если для подключения используется нестандартный порт, укажите его.

6. Если при подключении к хранилищу используется SSL, установите флажок **Использовать SSL**.
7. Если используется SSL и необходимо проверять используемый сертификат, установите флажок **Проверять подлинность SSL-сертификата**.
8. Если код региона отличается от `us-east-1`, в поле **Регион** введите код, предоставленный провайдером или указанный вами при создании бакета (например `ru-central-1`).
9. В полях **Логин** и **Пароль** введите данные статического ключа доступа, созданного для сервисного аккаунта.
10. В поле **Путь к папке** введите название бакета или объекта в бакете.

Название бакета может содержать только буквы латинского алфавита, цифры, точку, дефис и символ подчеркивания. В качестве разделителя для названий объектов в бакете используйте косую черту `/`.

11. Нажмите кнопку **Добавить источник**.

Источник добавлен в PT Email Security.

13.5. Внешняя система как ICAP-клиент

PT Email Security может проверять объекты, поступающие от внешних систем по протоколу ICAP. Для этого в PT Email Security настраивается ICAP-сервер, а внешняя система выступает в качестве ICAP-клиента.

Примечание. Ответ ICAP-сервера с результатом проверки объекта формируется только на основании статического анализа, сразу после его завершения. Если настроен поведенческий анализ, его результаты не влияют на работу ICAP-клиента, но доступны в карточке задания.

В зависимости от приобретенной вами лицензии PT Email Security и выбранных параметров работы ICAP-сервера проверка может выполняться в блокирующем режиме, режиме ожидания или в пассивном режиме:

- В блокирующем режиме при обнаружении угрозы ICAP-сервер не пропускает объект в информационную систему и отправляет в ответе ICAP-клиенту уведомление о блокировке объекта. Если в течение установленного тайм-аута ICAP-сервер не отправляет ответ, объект считается безопасным.
- В режиме ожидания при обнаружении угрозы ICAP-сервер отправляет ICAP-клиенту ответ с кодом 204 и добавляет в заголовок ответа X-Virus-ID краткое описание обнаруженной угрозы. Если в течение установленного тайм-аута ICAP-сервер не отправляет ответ, объект считается безопасным. Этот режим может использоваться для интеграции со сторонними системами, которые самостоятельно принимают решение о блокировке объектов.
- В пассивном режиме объект сразу пропускается в информационную систему, а не задерживается ICAP-сервером на время проверки, как в других режимах. Результаты проверки не влияют на работу ICAP-клиента, но доступны в карточке задания.

Внимание! Если в вашей информационной системе используется межсетевой экран или другие средства контроля сетевого трафика, требуется настроить в них правила, разрешающие передачу трафика через порт TCP 1344 от узла источника к основному узлу PT Email Security.

Для подключения внешней системы в PT Email Security необходимо добавить источник с типом **ICAP-сервер**.

Во внешней системе необходимо настроить ICAP-клиент для работы с ICAP-сервером, созданным при добавлении источника в PT Email Security:

- Необходимо указать ссылку для обращения к ICAP-серверу PT Email Security. Вид ссылки зависит от режима проверки объектов и режима работы ICAP-сервера.
- Если требуется отправлять IP-адрес пользователя, скачавшего файл, нужно настроить отправку поля заголовка X-Client-IP.
- Если требуется отправлять имя пользователя, скачавшего файл, нужно настроить отправку поля заголовка X-Client-Username.
- Если ICAP-клиент поддерживает режим ICAP Preview, рекомендуется отключить этот режим.

При настройке ICAP-клиента вам необходимо указать ссылку для обращения к ICAP-серверу PT Email Security. Вид ссылки зависит от режима проверки объектов и режима работы ICAP-сервера:

- Ссылки для проверки объектов в блокирующем режиме:
 - REQMOD: `icap://<IP-адрес>:<Порт>/scanrequest?modify=y&block-unwanted=<Блокировать потенциально опасные>&timeout=<Тайм-аут>`
 - RESPMOD: `icap://<IP-адрес>:<Порт>/scanresponse?modify=y&block-unwanted=<Блокировать потенциально опасные>&timeout=<Тайм-аут>`

Примечание. В параметре `block-unwanted` вы можете указать `y`, если необходимо блокировать потенциально опасные файлы, или `n` — если блокировать такие файлы не требуется (по умолчанию потенциально опасные файлы не блокируются). В параметре `timeout` вы можете указать тайм-аут ответа ICAP-сервера в секундах (по умолчанию 30 секунд).
- Ссылки для проверки объектов в режиме ожидания:
 - REQMOD: `icap://<IP-адрес>:<Порт>/scanrequest?modify=no&timeout=<Тайм-аут>`
 - RESPMOD: `icap://<IP-адрес>:<Порт>/scanresponse?modify=no&timeout=<Тайм-аут>`
- Ссылки для проверки объектов в пассивном режиме:
 - REQMOD: `icap://<IP-адрес>:<Порт>/bypass`
 - RESPMOD: `icap://<IP-адрес>:<Порт>/bypass`

Добавление источника в PT Email Security

► Чтобы добавить источник в PT Email Security:

1. В главном меню выберите **Источники**.
2. Нажмите кнопку **Добавить источник**.
3. В поле **Название** введите название источника, которое будет указано в свойствах полученных от него объектов.

Название должно содержать не менее пяти символов и быть уникальным среди названий всех источников. Название может содержать только строчные буквы латинского алфавита, цифры, дефис и при этом начинаться и заканчиваться только буквами.

4. В раскрывающемся списке **Тип** выберите **ICAP-сервер**.
5. Если необходимо, в поле **IP-адреса ICAP-сервера** введите дополнительные адреса.

Примечание. В поле указан IP-адрес ICAP-сервера, создаваемого в PT Email Security. Он понадобится вам при настройке источника.

6. Если необходимо, измените стандартный порт подключения к ICAP-серверу.

Внимание! Указанный порт не должен использоваться другими источниками для проверки, службами или приложениями ОС.

7. Если необходимо принимать объекты только с определенных адресов, включите фильтрацию входящих подключений и укажите IP-адреса разрешенных узлов или подсетей.
8. Нажмите кнопку **Добавить источник**.

Источник добавлен в PT Email Security.

13.6. Внешняя система через API

PT Email Security может проверять объекты, поступающие от внешних систем через публичный API. Проверка выполняется в режиме ожидания.

Внимание! Если в вашей информационной системе используется межсетевой экран или другие средства контроля сетевого трафика, требуется настроить в них правила, разрешающие передачу трафика через порты TCP 80, 443 от узла источника к основному узлу PT Email Security.

Примечание. На размер файлов, поступающих на проверку в PT Email Security через публичный API, установлено ограничение в 1 ГБ. При необходимости вы можете изменить этот размер командой `sudo ptmsctl system components set -c nginx -p max_file_size=<Размер в МБ>`.

PT Email Security поддерживает два способа проверки объектов, поступающих от внешних систем через публичный API: когда параметры проверки передаются в запросе вместе с каждым объектом и когда объекты проверяются с общими параметрами проверки, добавленного в PT Email Security источника.

Для подключения внешней системы при проверке объектов с передаваемыми параметрами необходимо:

- В PT Email Security выпустить токен доступа к публичному API с разрешенным действием **Проверка с передаваемыми параметрами**.
- Во внешней системе настроить отправку объектов в PT Email Security через публичный API. Каждый запрос должен содержать в заголовке X-API-Key выпущенный токен доступа.

Для подключения внешней системы при проверке объектов с параметрами источника необходимо:

- В PT Email Security выпустить токен доступа к публичному API с разрешенным действием **Проверка с параметрами источника**.
- Добавить в PT Email Security источник с типом **API с выбранными параметрами проверки**.
- Во внешней системе настроить отправку объектов в PT Email Security через публичный API. Каждый запрос должен содержать в заголовке X-API-Key выпущенный токен доступа.

Добавление источника в PT Email Security

► Чтобы добавить источник в PT Email Security:

1. В главном меню выберите **Источники**.
2. Нажмите кнопку **Добавить источник**.
3. В поле **Название** введите название источника, которое будет указано в свойствах полученных от него объектов.

Название должно содержать не менее пяти символов и быть уникальным среди названий всех источников. Название может содержать только строчные буквы латинского алфавита, цифры, дефис и при этом начинаться и заканчиваться только буквами.

4. В раскрывающемся списке **Тип** выберите **API с выбранными параметрами проверки**.
5. В раскрывающемся списке **Токен доступа** выберите токен доступа к публичному API.
6. Нажмите кнопку **Добавить источник**.

Источник добавлен в PT Email Security.

13.7. Почтовый шлюз безопасности

При установке и подключении почтового шлюза безопасности письма от SMTP-клиентов принимаются шлюзом и отправляются на проверку в PT Email Security, после чего доставляются получателям через указанные в правилах маршрутизации почтовые серверы.

Внимание! Если в вашей информационной системе используется межсетевой экран или другие средства контроля сетевого трафика, необходимо настроить в них правила, разрешающие передачу трафика от почтового шлюза безопасности к основному узлу PT Email Security на порты 25 и 50052.

Для подключения источника к PT Email Security необходимо:

1. Добавить в PT Email Security источник с типом **Почтовый шлюз безопасности**.
2. Развернуть почтовый шлюз безопасности на отдельном узле.
3. Настроить в сетевой инфраструктуре организации маршрутизацию писем через почтовый шлюз безопасности.
4. Настроить в PT Email Security отправку проверенных писем:
 - Если используется несколько почтовых серверов, добавить правила маршрутизации.
 - Если используются непубличные почтовые серверы и требуется TLS-шифрование с проверкой сертификата, добавить корневой сертификат центра сертификации вашей организации.
 - Если на почтовых серверах поддерживается проверка адресов получателей, включить такую проверку для добавленного источника.

В этом разделе

[Добавление источника в PT Email Security \(см. раздел 13.7.1\)](#)

[Развертывание почтового шлюза безопасности \(см. раздел 13.7.2\)](#)

[Добавление правил маршрутизации проверенных писем \(см. раздел 13.7.3\)](#)

[Добавление доверенных сертификатов \(см. раздел 13.7.4\)](#)

[Включение проверки адресов получателей \(см. раздел 13.7.5\)](#)

13.7.1. Добавление источника в PT Email Security

► Чтобы добавить источник в PT Email Security:

1. В главном меню выберите **Источники**.
2. Нажмите кнопку **Добавить источник**.
3. В поле **Название** введите название источника, которое будет указано в свойствах полученных от него объектов.

Название должно содержать не менее пяти символов и быть уникальным среди названий всех источников. Название может содержать только строчные буквы латинского алфавита, цифры, дефис и при этом начинаться и заканчиваться только буквами.

4. В раскрывающемся списке **Тип** выберите **Почтовый шлюз безопасности**.
5. В блоке **Параметры подключения** настройте параметры SMTP-сервера, создаваемого почтовым шлюзом для приема писем:
 - Если необходимо, в поле **IP-адреса SMTP-сервера** введите дополнительные адреса.

Примечание. В поле указан IP-адрес SMTP-сервера, создаваемого в PT Email Security. Он понадобится вам при настройке почтового шлюза.

 - Если необходимо, измените стандартный порт подключения к серверу.

Внимание! Указанный порт не должен использоваться другими источниками для проверки, службами или приложениями ОС.
6. Если требуется, в блоке параметров **Правила маршрутизации почтового трафика** в раскрывающемся списке **Доверенные сертификаты TLS-шифрования** выберите для всех правил маршрутизации, какой набор доверенных сертификатов будет использоваться для проверки сертификатов почтовых серверов:
 - Если только доверенные сертификаты из внутреннего хранилища PT Email Security, выберите **Пользовательские**.
 - Если сертификаты из внутреннего хранилища и глобальные сертификаты, доступные внутри докер-контейнеров PT Email Security, выберите **Глобальные и пользовательские**.
7. Добавьте правило маршрутизации по умолчанию и укажите в нем параметры сервера для отправки писем и уведомлений о результатах проверки:
 - Нажмите кнопку **Добавить**.
 - В блоке параметров **Требования к TLS-шифрованию** укажите для всех почтовых серверов в правиле, требуется ли TLS-шифрование.
 - Если при шифровании требуется проверять сертификат почтового сервера, установите флажок **Проверять сертификат**.
 - В поле **Доменное имя или IP-адрес** введите адрес и порт сервера.
 - Если в вашей организации используется несколько почтовых серверов, в поле **Приоритет** введите число, соответствующее приоритету сервера с указанным адресом.

Примечание. Вы можете указать число от 1 до 65535. Чем меньше число, тем выше приоритет сервера. Письма будут отправляться на активные серверы с наибольшим приоритетом. Если для серверов указан одинаковый приоритет, почтовый трафик балансируется между ними поровну.

- В раскрывающемся списке **Режим запуска TLS-шифрования** выберите режим запуска шифрования для этого сервера.
- Если для доступа к серверу требуется аутентификация, включите использование аутентификации и в раскрывающемся списке **Тип аутентификации** выберите ее тип.

Примечание. При автоматическом выборе типа аутентификации PT Email Security выбирает наиболее безопасный тип из предложенных почтовым сервером.

- Если используется аутентификация, в поля **Логин** и **Пароль** введите учетные данные для доступа к серверу.
- Если в вашей организации используется несколько почтовых серверов, по кнопке **Добавить сервер** добавьте для них блоки параметров и настройте аналогичным образом.
- Нажмите кнопку **Добавить**.

8. Нажмите кнопку **Добавить источник**.

13.7.2. Развертывание почтового шлюза безопасности

Внимание! Если в вашей информационной системе используется межсетевой экран или другие средства контроля сетевого трафика, требуется настроить в них правила, разрешающие передачу трафика от узлов SMTP-клиентов к узлу почтового шлюза безопасности на порт TCP 25.

Почтовый шлюз безопасности может быть развернут как на физическом сервере, так и в виртуальной среде. При развертывании почтового шлюза безопасности на узле вам необходимо:

1. Установить почтовый транспортный агент Postfix.
2. Установить агент почтового шлюза безопасности.
3. Настроить параметры почтового шлюза.
4. Добавить для почтового шлюза сертификат PT Email Security.
5. Установить сертификат почтового шлюза в PT Email Security.

Аппаратные требования

Минимальные аппаратные требования к узлу для установки почтового шлюза безопасности указаны в таблице.

Таблица 4. Минимальные аппаратные требования

Компонент	Требование
Центральный процессор 2,2 ГГц, количество потоков	2
Память ОЗУ, ГБ	4

Компонент	Требование
SSD, ГБ	40

Программные требования

Установка почтового шлюза безопасности возможна на узле с 64-разрядной операционной системой Debian GNU/Linux 12.

Внимание! Каталог `/var` должен быть вынесен в отдельный раздел диска объемом не менее 30 ГБ.

Примечание. Для установки почтового шлюза безопасности в виртуальной среде необходимо использовать гипервизор VMware ESXi версии 6.0 или выше с аппаратным обеспечением версии 11 или выше.

К настройке операционной системы на узле для установки почтового шлюза безопасности выдвигаются следующие требования:

- Установлено точное время и настроена синхронизация с NTP-сервером.
- Настроено подключение к DNS-серверу.
- Настроен менеджер пакетов APT.
- Установлена программа `sudo`. Пользователь, от имени которого выполняется установка, добавлен в группу `sudo`.

Установка почтового транспортного агента Postfix

- Чтобы установить на узле Postfix,

выполните команду:

```
sudo apt update && sudo apt install postfix -y
```

Установка агента почтового шлюза безопасности

Для получения установочного пакета агента почтового шлюза безопасности вам необходимо обратиться в техническую поддержку Positive Technologies.

- Чтобы установить на узле агент почтового шлюза безопасности:

1. Скопируйте установочный пакет в любой каталог на основном узле.
2. Перейдите в этот каталог.
3. Выполните команду:

```
sudo dpkg -i espa.deb
```

Настройка параметров почтового шлюза безопасности

► Чтобы настроить параметры шлюза безопасности:

1. Откройте файл `/etc/espa/config.toml`.
2. Укажите параметры:
 - В секции `management` в параметре `product_ip` укажите адрес основного узла PT Email Security:


```
[management]
product_ip = "<IP-адрес основного узла PT Email Security>"
```
 - В секции `postfix` в параметре `host_name` укажите доменное имя, которое будет доступно SMTP-клиенту при запросе на подключение к почтовому шлюзу:


```
[postfix]
host_name = "<Доменное имя шлюза>"
```
 - В параметре `relayhost` укажите IP-адрес и порт SMTP-сервера, указанные при добавлении источника в PT Email Security:


```
relayhost = "<IP-адрес SMTP-сервера>:<Порт>"
```

Например:

```
[management]
product_ip = "192.0.1.1"
[postfix]
host_name = "example.gateway.name"
relayhost = "192.0.1.1:25"
```
3. Сохраните изменения и закройте файл.
4. Перезапустите службу конфигуратора шлюза:


```
sudo systemctl restart espa-configurator
```

Добавление сертификата PT Email Security для почтового шлюза безопасности

Инструкцию необходимо выполнить на основном узле PT Email Security.

► Чтобы выгрузить данные сертификата из PT Email Security:

1. Создайте в любом каталоге файл `product_ca.crt`.
2. Выполните команду:


```
sudo kubectl --kubeconfig=/etc/kubernetes/admin.conf -n ptms get secrets ms-public-k8s-cert -o=jsonpath="{.data.ca\.crt}" | base64 -d
```
3. Скопируйте результат выполнения команды в файл `product_ca.crt`.
4. Сохраните изменения и закройте файл.

Инструкцию необходимо выполнить на узле почтового шлюза безопасности.

► Чтобы добавить сертификат для почтового шлюза безопасности:

1. Скопируйте файл `product_ca.crt` в каталог `/etc/esp/`.

2. Перезапустите службу configurator шлюза:

```
sudo systemctl restart esp-configurator
```

Установка сертификата почтового шлюза безопасности в PT Email Security

Сертификат почтового шлюза безопасности `ca.crt` находится на узле шлюза в каталоге `/etc/esp/certs`.

Инструкцию необходимо выполнить на основном узле PT Email Security.

► Чтобы установить сертификата почтового шлюза безопасности в PT Email Security:

1. Скопируйте файл сертификата `ca.crt` в любой каталог на узле.

2. Выполните команду:

```
sudo ptmsctl mail esp add --ip <IP-адрес узла шлюза> --ca <Путь к файлу ca.crt> --entrypoint-id <Название источника в PT Email Security>
```

Например:

```
sudo ptmsctl mail esp add --ip 192.0.2.15 --ca /home/user/ca.crt --entrypoint-id example-source-name
```

13.7.3. Добавление правил маршрутизации проверенных писем

Если необходимо использовать различные почтовые серверы в зависимости от домена в адресе электронной почты получателя, вы можете настроить в PT Email Security [правила маршрутизации проверенных писем](#) (см. раздел 12.2).

► Чтобы добавить правило маршрутизации:

1. В главном меню выберите **Источники**.
2. В панели с информацией об источнике перейдите по ссылке **Параметры источника**.
3. В блоке параметров **Правила маршрутизации почтового трафика** нажмите кнопку **Добавить**.
4. В поле **Домен электронной почты получателя** введите доменную часть адреса электронной почты получателей, для которых необходимо настроить правило.

С помощью звездочки вы можете задать маску для доменной части адреса получателей писем, если доменная часть содержит поддомены третьего уровня или выше. Например, правило с маской *.example.com будет применяться и для адресов с доменной частью example.com, sub_1.example.com, sub_2.example.com, и для адресов с доменной частью, содержащей поддомены более высоких уровней.

Примечание. Если доменная часть адреса получателя соответствует нескольким правилам маршрутизации, будет использовано то правило, в котором указан наиболее точный адрес. При этом более высокий приоритет имеют правила, в которых не используются маски.

5. В блоке параметров **Требования к TLS-шифрованию** укажите для всех почтовых серверов в правиле, требуется ли TLS-шифрование.
6. Если при шифровании требуется проверять сертификат почтового сервера, установите флажок **Проверять сертификат**.
7. Если необходимо перенаправлять письма согласно MX-записям, выберите способ маршрутизации **По MX-записям**.

Внимание! Письмо не будет отправлено, если в DNS отсутствует подходящая MX- или A-запись для указанного домена.

8. Если необходимо перенаправлять письма на определенный почтовый сервер, выберите способ маршрутизации **По адресам почтовых серверов** и укажите параметры сервера:
 - В поле **Доменное имя или IP-адрес** введите адрес и порт сервера.
 - Если в вашей организации используется несколько почтовых серверов, в поле **Приоритет** введите число, соответствующее приоритету сервера с указанным адресом.

Примечание. Вы можете указать число от 1 до 65535. Чем меньше число, тем выше приоритет сервера. Письма будут отправляться на активные серверы с наибольшим приоритетом. Если для серверов указан одинаковый приоритет, почтовый трафик балансируется между ними поровну.

- В раскрывающемся списке **Режим запуска TLS-шифрования** выберите режим запуска шифрования для этого сервера.
- Если для доступа к серверу требуется аутентификация, включите использование аутентификации и в раскрывающемся списке **Тип аутентификации** выберите ее тип.

Примечание. При автоматическом выборе типа аутентификации PT Email Security выбирает наиболее безопасный тип из предложенных почтовым сервером.

- Если используется аутентификация, в поля **Логин** и **Пароль** введите учетные данные для доступа к серверу.
- Если в вашей организации используется несколько почтовых серверов, по кнопке **Добавить сервер** добавьте для них блоки параметров и настройте аналогичным образом.

9. Нажмите кнопку **Добавить**.

10. Нажмите кнопку **Сохранить**.

Правило маршрутизации добавлено.

13.7.4. Добавление доверенных сертификатов

Если при отправке проверенных писем вы планируете использовать TLS-шифрование с проверкой сертификата, при проверке сертификатов почтовых серверов будут использоваться следующие сертификаты:

- Для публичных SMTP-серверов — сертификаты доверенных центров сертификации, доступные внутри докер-контейнеров PT Email Security.
- Для непубличных SMTP-серверов вашей организации — доверенные сертификаты центров сертификации вашей организации. Корневые сертификаты этих центров необходимо добавить в PT Email Security.

Инструкции необходимо выполнять на основном узле PT Email Security. Поддерживаются только сертификаты формата PEM.

- ▶ Чтобы добавить сертификат в PT Email Security,

выполните команду:

```
sudo ptmsctl system trusted-certs add --name <Название сертификата> --path <Полный путь к файлу сертификата>
```

Например:

```
sudo ptmsctl system trusted-certs add --name example_cert --path /etc/tls/certs/rootCA.crt
```

- ▶ Чтобы просмотреть список добавленных в PT Email Security сертификатов,

выполните команду:

```
sudo ptmsctl system trusted-certs list
```

Примечание. Вы можете просмотреть информацию об отдельном сертификате, выполнив команду `sudo ptmsctl system trusted-certs view --name <Название сертификата>`.

- ▶ Чтобы удалить сертификат из PT Email Security,

выполните команду:

```
sudo ptmsctl system trusted-certs delete --name <Название сертификата>
```

Например:

```
sudo ptmsctl system trusted-certs delete --name example_cert
```

13.7.5. Включение проверки адресов получателей

Перед отправкой проверенных писем PT Email Security может проверять адреса получателей на принимающих почтовых серверах с помощью SMTP-команды **VERFY** (согласно спецификации RFC 5321). По умолчанию эта проверка отключена, поскольку на некоторых почтовых серверах выполнение этой команды может быть заблокировано по соображениям безопасности. Вы можете включить для источника проверку адресов получателей, если для него добавлено хотя бы одно правило маршрутизации или указано более одного почтового сервера. Инструкцию необходимо выполнить на основном узле PT Email Security.

- Чтобы включить проверку адресов получателей для источника,

выполните команду:

```
sudo ptmsctl system components config patch --component <Название источника> --toml "[smtp_client_config.verify_recipients]
enabled = true
"
```

13.8. «Код безопасности», «Континент» 4.1

При подключении источника объекты от межсетевого экрана «Континент» отправляются на проверку в PT Email Security по протоколу ICAP. В зависимости от приобретенной вами лицензии и выбранных параметров работы ICAP-сервера PT Email Security проверка может выполняться в режиме ожидания, в пассивном или блокирующем режиме.

Внимание! Если в вашей информационной системе используется межсетевой экран или другие средства контроля сетевого трафика, требуется настроить в них правила, разрешающие передачу трафика через порт TCP 1344 от узла источника к основному узлу PT Email Security.

Для подключения источника к PT Email Security необходимо:

- Добавить в PT Email Security источник с типом **ICAP-сервер**.
- На межсетевом экране «Континент» настроить ICAP-клиент для работы с ICAP-сервером PT Email Security.

Добавление источника в PT Email Security

- Чтобы добавить источник в PT Email Security:

1. В главном меню выберите **Источники**.
2. Нажмите кнопку **Добавить источник**.
3. В поле **Название** введите название источника, которое будет указано в свойствах полученных от него объектов.

Название должно содержать не менее пяти символов и быть уникальным среди названий всех источников. Название может содержать только строчные буквы латинского алфавита, цифры, дефис и при этом начинаться и заканчиваться только буквами.

4. В раскрывающемся списке **Тип** выберите **ICAP-сервер**.
5. Если необходимо, в поле **IP-адреса ICAP-сервера** введите дополнительные адреса.

Примечание. В поле указан IP-адрес ICAP-сервера, создаваемого в PT Email Security. Он понадобится вам при настройке источника.

6. Если необходимо, измените стандартный порт подключения к ICAP-серверу.
Внимание! Указанный порт не должен использоваться другими источниками для проверки, службами или приложениями ОС.
7. Если необходимо принимать объекты только с определенных адресов, включите фильтрацию входящих подключений и укажите IP-адреса разрешенных узлов или подсетей.
8. Нажмите кнопку **Добавить источник**.

Источник добавлен в PT Email Security.

Настройка источника

Для межсетевого экрана «Континент» необходимо настроить ICAP-клиент для работы с ICAP-сервером, созданным при добавлении источника в PT Email Security. Дополнительную информацию о настройке межсетевого экрана «Континент» вы можете получить на сайте securitycode.ru.

При настройке ICAP-клиента вам необходимо указать ссылки для обращения к ICAP-серверу PT Email Security. Вид ссылки зависит от режима проверки объектов и режима работы ICAP-сервера:

- Ссылки для проверки объектов в блокирующем режиме:
 - REQMOD: /scanrequest?modify=y&block-unwanted=<Блокировать потенциально опасные>&timeout=5
 - RESPMOD: /scanresponse?modify=y&block-unwanted=<Блокировать потенциально опасные>&timeout=5

Примечание. В параметре `block-unwanted` вы можете указать `y`, если необходимо блокировать потенциально опасные файлы, или `n` — если блокировать такие файлы не требуется (по умолчанию потенциально опасные файлы не блокируются). В параметре `timeout` вы можете изменить тайм-аут ответа ICAP-сервера в секундах.

— Ссылки для проверки объектов в режиме ожидания:

- REQMOD: `/scanrequest?modify=no&timeout=5`
- RESPMOD: `/scanresponse?modify=no&timeout=5`

— Ссылки для проверки объектов в пассивном режиме:

- REQMOD: `/bypass`
- RESPMOD: `/bypass`

► Чтобы настроить ICAP-клиент:

1. Запустите «Менеджер конфигурации» межсетевого экрана «Континент».
2. Подключитесь к центру управления сетью (ЦУС) под учетной записью администратора.
3. В левой части окна нажмите кнопку **Контроль доступа**.
4. В панели **Навигация** выберите **Межсетевой экран** → **Группы Web/FTP-фильтров** → **ICAP-серверы**.
5. В панели инструментов нажмите кнопку **ICAP-сервер**.
Откроется окно **ICAP-сервер** на вкладке **Общие сведения**.
6. Укажите информацию об ICAP-сервере:

- В поле **Название** введите произвольное название ICAP-сервера.
- В поле **Адрес сервера** введите адрес ICAP-сервера PT Email Security.
- Если используемый порт отличается от 1344, в поле **Порт** введите номер порта.
- В поле **Тайм-аут опроса ICAP-сервера** введите 75.

Внимание! Тайм-аут опроса ICAP-сервера должен быть на 5–15 секунд больше значения параметра `timeout` в ссылке для обращения к ICAP-серверу PT Email Security.

- Если политика безопасности вашей организации позволяет пропускать непроверенные объекты, установите флажок **Пропускать при недоступности сервера**.
7. Выберите вкладку **Дополнительно**.
 8. Укажите ссылки для обращения к ICAP-серверу PT Email Security для выбранного вами режима проверки объектов:
 - Установите флажок **Режим модификации запроса** и в поле **Путь к службе** введите ссылку для REQMOD.
 - Установите флажок **Режим модификации ответа** и в поле **Путь к службе** введите ссылку на ICAP-сервер PT Email Security для RESPMOD.

- Установите флажок **Отправлять имя пользователя** и в поле **Заголовок** введите X-Client-Username.
 - Установите флажок **Отправлять IP-адрес** и в поле **Заголовок** введите X-Client-IP.
9. Если требуется отправлять на проверку только определенные типы файлов, выберите вкладку **Фильтры** и по кнопке  добавьте MIME-типы файлов.
10. Нажмите кнопку **ОК**.
11. В панели **Навигация** выберите **Межсетевой экран** → **Группы Web/FTP-фильтров** → **Профили Web/FTP-фильтрации**.
12. Добавьте профиль для фильтрации HTTP-трафика:
- В панели инструментов нажмите кнопку **Профиль Web/FTP-фильтрации**.
 - В поле **Название** введите HTTP.
 - В раскрывающемся списке **Схема** выберите HTTP.
 - В меню кнопки  выберите **ICAP-серверы**.
 - В открывшемся окне выберите добавленный ранее ICAP-сервер.
 - После добавления сервера в списке **Группы Web/FTP-фильтров** в столбце **Действие** выберите режим проверки объектов.
 - Нажмите кнопку **ОК**.
13. Добавьте профиль для фильтрации HTTPS-трафика:
- В панели инструментов нажмите кнопку **Профиль Web/FTP-фильтрации**.
 - В поле **Название** введите HTTPS.
 - В раскрывающемся списке **Схема** выберите HTTPS.
 - В меню кнопки  выберите **ICAP-серверы**.
 - В открывшемся окне выберите добавленный ранее ICAP-сервер.
 - После добавления сервера в списке **Группы Web/FTP-фильтров** в столбце **Действие** выберите режим проверки объектов.
 - Нажмите кнопку **ОК**.
14. В панели **Навигация** выберите **Межсетевой экран**.
15. В панели инструментов нажмите кнопку **Установить**.
- ICAP-клиент настроен.

13.9. Exim 4 в режиме фильтрации

При подключении источника письма с сервера Exim отправляются на проверку в PT Email Security, после чего возвращаются обратно для дальнейшей доставки.

Внимание! Если в вашей информационной системе используется межсетевой экран или другие средства контроля сетевого трафика, требуется настроить в них правила, разрешающие передачу трафика через порт TCP 25 от почтового сервера к основному узлу PT Email Security.

Для подключения источника к PT Email Security необходимо:

1. Добавить в PT Email Security источник с типом **Почтовый сервер в режиме фильтрации** или **Почтовый сервер в режиме фильтрации (MTA)**.
2. Настроить в PT Email Security отправку проверенных писем:
 - Если используется несколько почтовых серверов, добавить правила маршрутизации.
 - Если используются непубличные почтовые серверы и требуется TLS-шифрование с проверкой сертификата, добавить корневой сертификат центра сертификации вашей организации.
 - Если на почтовых серверах поддерживается проверка адресов получателей, включить такую проверку для добавленного источника.
3. На сервере Exim настроить маршрутизацию писем через PT Email Security.

Добавление источника в PT Email Security

► Чтобы добавить источник в PT Email Security:

1. В главном меню выберите **Источники**.
2. Нажмите кнопку **Добавить источник**.
3. В поле **Название** введите название источника, которое будет указано в свойствах полученных от него объектов.

Название должно содержать не менее пяти символов и быть уникальным среди названий всех источников. Название может содержать только строчные буквы латинского алфавита, цифры, дефис и при этом начинаться и заканчиваться только буквами.

4. В раскрывающемся списке **Тип** выберите:
 - Если для работы с письмами от источника необходимо использовать встроенный в PT Email Security почтовый транспортный агент, выберите **Почтовый сервер в режиме фильтрации (MTA)**.
 - Если в этом нет необходимости, выберите **Почтовый сервер в режиме фильтрации**.

5. Если вы выбрали тип **Почтовый сервер в режиме фильтрации (MTA)**, в блоке параметров **Режим обработки писем** выберите режим:
 - Если хранение и доставку проверенных писем должен контролировать PT Email Security, выберите **Асинхронный**.
 - Если это должен делать почтовый сервер, выберите **Синхронный**.
6. В блоке **Параметры подключения** настройте параметры SMTP-сервера, создаваемого в PT Email Security для приема писем:
 - Если необходимо, в поле **IP-адреса SMTP-сервера** введите дополнительные адреса.

Примечание. В поле указан IP-адрес SMTP-сервера, создаваемого в PT Email Security. Он понадобится вам при настройке источника.

- Если необходимо, измените стандартный порт подключения к серверу.
- **Внимание!** Указанный порт не должен использоваться другими источниками для проверки, службами или приложениями ОС.
- Если при подключении используется протокол SSL, установите флажок **Подключаться по SSL**.

Примечание. При снятом флажке передаваемые данные зашифровываются при помощи расширения STARTTLS. Если почтовый сервер организации не поддерживает STARTTLS, данные передаются без шифрования.

7. Если необходимо принимать письма только с определенных адресов, включите фильтрацию входящих подключений и укажите IP-адреса разрешенных узлов или подсетей.
8. Если требуется, в блоке параметров **Правила маршрутизации почтового трафика** в раскрывающемся списке **Доверенные сертификаты TLS-шифрования** выберите для всех правил маршрутизации, какой набор доверенных сертификатов будет использоваться для проверки сертификатов почтовых серверов:
 - Если только доверенные сертификаты из внутреннего хранилища PT Email Security, выберите **Пользовательские**.
 - Если сертификаты из внутреннего хранилища и глобальные сертификаты, доступные внутри докер-контейнеров PT Email Security, выберите **Глобальные и пользовательские**.
9. Добавьте правило маршрутизации по умолчанию и укажите в нем параметры сервера для отправки писем и уведомлений о результатах проверки:
 - Нажмите кнопку **Добавить**.
 - В блоке параметров **Требования к TLS-шифрованию** укажите для всех почтовых серверов в правиле, требуется ли TLS-шифрование.
 - Если при шифровании требуется проверять сертификат почтового сервера, установите флажок **Проверять сертификат**.

- В поле **Доменное имя или IP-адрес** введите адрес и порт сервера.
- Если в вашей организации используется несколько почтовых серверов, в поле **Приоритет** введите число, соответствующее приоритету сервера с указанным адресом.

Примечание. Вы можете указать число от 1 до 65535. Чем меньше число, тем выше приоритет сервера. Письма будут отправляться на активные серверы с наибольшим приоритетом. Если для серверов указан одинаковый приоритет, почтовый трафик балансируется между ними поровну.

- В раскрывающемся списке **Режим запуска TLS-шифрования** выберите режим запуска шифрования для этого сервера.
 - Если для доступа к серверу требуется аутентификация, включите использование аутентификации и в раскрывающемся списке **Тип аутентификации** выберите ее тип.
- Примечание.** При автоматическом выборе типа аутентификации PT Email Security выбирает наиболее безопасный тип из предложенных почтовым сервером.
- Если используется аутентификация, в поля **Логин** и **Пароль** введите учетные данные для доступа к серверу.
 - Если в вашей организации используется несколько почтовых серверов, по кнопке **Добавить сервер** добавьте для них блоки параметров и настройте аналогичным образом.
 - Нажмите кнопку **Добавить**.

10. Нажмите кнопку **Добавить источник**.

Источник добавлен в PT Email Security.

Добавление правила маршрутизации проверенных писем в PT Email Security

Если необходимо использовать различные почтовые серверы в зависимости от домена в адресе электронной почты получателя, вы можете настроить в PT Email Security [правила маршрутизации проверенных писем](#) (см. раздел 12.2).

► Чтобы добавить правило маршрутизации:

1. В главном меню выберите **Источники**.
2. В панели с информацией об источнике перейдите по ссылке **Параметры источника**.
3. В блоке параметров **Правила маршрутизации почтового трафика** нажмите кнопку **Добавить**.
4. В поле **Домен электронной почты получателя** введите доменную часть адреса электронной почты получателей, для которых необходимо настроить правило.

С помощью звездочки вы можете задать маску для доменной части адреса получателей писем, если доменная часть содержит поддомены третьего уровня или выше. Например, правило с маской *.example.com будет применяться и для адресов с доменной частью example.com, sub_1.example.com, sub_2.example.com, и для адресов с доменной частью, содержащей поддомены более высоких уровней.

Примечание. Если доменная часть адреса получателя соответствует нескольким правилам маршрутизации, будет использовано то правило, в котором указан наиболее точный адрес. При этом более высокий приоритет имеют правила, в которых не используются маски.

5. В блоке параметров **Требования к TLS-шифрованию** укажите для всех почтовых серверов в правиле, требуется ли TLS-шифрование.
6. Если при шифровании требуется проверять сертификат почтового сервера, установите флажок **Проверять сертификат**.
7. Если необходимо перенаправлять письма согласно MX-записям, выберите способ маршрутизации **По MX-записям**.

Внимание! Письмо не будет отправлено, если в DNS отсутствует подходящая MX- или A-запись для указанного домена.

8. Если необходимо перенаправлять письма на определенный почтовый сервер, выберите способ маршрутизации **По адресам почтовых серверов** и укажите параметры сервера:
 - В поле **Доменное имя или IP-адрес** введите адрес и порт сервера.
 - Если в вашей организации используется несколько почтовых серверов, в поле **Приоритет** введите число, соответствующее приоритету сервера с указанным адресом.

Примечание. Вы можете указать число от 1 до 65535. Чем меньше число, тем выше приоритет сервера. Письма будут отправляться на активные серверы с наибольшим приоритетом. Если для серверов указан одинаковый приоритет, почтовый трафик балансируется между ними поровну.

- В раскрывающемся списке **Режим запуска TLS-шифрования** выберите режим запуска шифрования для этого сервера.
- Если для доступа к серверу требуется аутентификация, включите использование аутентификации и в раскрывающемся списке **Тип аутентификации** выберите ее тип.

Примечание. При автоматическом выборе типа аутентификации PT Email Security выбирает наиболее безопасный тип из предложенных почтовым сервером.

- Если используется аутентификация, в поля **Логин** и **Пароль** введите учетные данные для доступа к серверу.
- Если в вашей организации используется несколько почтовых серверов, по кнопке **Добавить сервер** добавьте для них блоки параметров и настройте аналогичным образом.

9. Нажмите кнопку **Добавить**.

10. Нажмите кнопку **Сохранить**.

Правило маршрутизации добавлено.

Добавление доверенных сертификатов в PT Email Security

Если при отправке проверенных писем вы планируете использовать TLS-шифрование с проверкой сертификата, при проверке сертификатов почтовых серверов будут использоваться следующие сертификаты:

- Для публичных SMTP-серверов — сертификаты доверенных центров сертификации, доступные внутри докер-контейнеров PT Email Security.
- Для непубличных SMTP-серверов вашей организации — доверенные сертификаты центров сертификации вашей организации. Корневые сертификаты этих центров необходимо добавить в PT Email Security.

Инструкции необходимо выполнять на основном узле PT Email Security. Поддерживаются только сертификаты формата PEM.

- ▶ Чтобы добавить сертификат в PT Email Security,

выполните команду:

```
sudo ptmsctl system trusted-certs add --name <Название сертификата> --path <Полный путь к файлу сертификата>
```

Например:

```
sudo ptmsctl system trusted-certs add --name example_cert --path /etc/tls/certs/rootCA.crt
```

- ▶ Чтобы просмотреть список добавленных в PT Email Security сертификатов,

выполните команду:

```
sudo ptmsctl system trusted-certs list
```

Примечание. Вы можете просмотреть информацию об отдельном сертификате, выполнив команду `sudo ptmsctl system trusted-certs view --name <Название сертификата>`.

- ▶ Чтобы удалить сертификат из PT Email Security,

выполните команду:

```
sudo ptmsctl system trusted-certs delete --name <Название сертификата>
```

Например:

```
sudo ptmsctl system trusted-certs delete --name example_cert
```

Включение проверки адресов получателей

Перед отправкой проверенных писем PT Email Security может проверять адреса получателей на принимающих почтовых серверах с помощью SMTP-команды VRFY (согласно спецификации RFC 5321). По умолчанию эта проверка отключена, поскольку на некоторых почтовых серверах выполнение этой команды может быть заблокировано по соображениям безопасности. Вы можете включить для источника проверку адресов получателей, если для него добавлено хотя бы одно правило маршрутизации или указано более одного почтового сервера. Инструкцию необходимо выполнить на основном узле PT Email Security.

- ▶ Чтобы включить проверку адресов получателей для источника,

выполните команду:

```
sudo ptmsctl system components config patch --component <Название источника> --toml "[smtp_client_config.verify_recipients]
enabled = true
"
```

Настройка источника

На сервере Exim необходимо настроить маршрутизацию писем через PT Email Security.

Инструкция разработана для Exim версии 4 с отдельными файлами конфигурации. Если вы используете единый конфигурационный файл, указанные в инструкции строки необходимо добавлять в этот файл. Дополнительную информацию вы можете получить на сайте exim.org.

- ▶ Чтобы настроить маршрутизацию писем через PT Email Security:

1. Создайте транспорт `remote_smtp_check`:

- Создайте файл `45_exim4-config_remote_smtp_check`:

```
sudo nano etc/exim4/conf.d/transport/45_exim4-config_remote_smtp_check
```

- Добавьте в файл строки, указав порт SMTP-сервера PT Email Security:

```
remote_smtp_check:
  driver = smtp
  port = <Порт PT Email Security>
  delay_after_cutoff = false
```

- Если необходимо увеличить тайм-ауты SMTP-сессии, добавьте в файл в секцию `remote_smtp_check` строки:

```
command_timeout = 25m
final_timeout = 30m
```

Примечание. Тайм-ауты SMTP-сессии должны превышать время проверки письма в PT Email Security. Если в вашей организации разрешена отправка писем с вложениями большого размера (сотни мегабайт), рекомендуется увеличить тайм-ауты SMTP-сессии.

- Сохраните изменения и закройте файл.

2. Настройте правило маршрутизации почтового трафика Exim:

- Создайте файл `050_exim4-config_ptes`.

```
sudo nano /etc/exim4/conf.d/router/050_exim4-config_ptes
```

- Добавьте в файл строки, указав порт сервера Exim для проверенных писем и адрес SMTP-сервера PT Email Security:

```
send_to_check:
    driver = manualroute
    condition = ${if eq {$interface_port}{<Порт Exim>}{no}{yes}}
    transport = remote_smtp_check
    route_list = * <IP-адрес PT Email Security>
    address_test = false
```

- Сохраните изменения и закройте файл.

Внимание! Правило маршрутизации `send_to_check` должно иметь самый высокий приоритет. Для этого в каталоге `/etc/exim4/conf.d/router` файл `050_exim4-config_scanner` должен располагаться сразу после файла `00_exim4-config_header`.

3. Добавьте список контроля доступа (ACL) для писем от PT Email Security:

- Создайте файл `25_exim4-config_check_host`:

```
sudo nano /etc/exim4/conf.d/acl/25_exim4-config_check_host
```

- Добавьте в файл строки, указав порт Exim для проверенных писем и адрес SMTP-сервера PT Email Security:

```
acl_check_host:
    deny
        message = Untrusted sender host
        condition = ${if eq {$interface_port}{<Порт Exim>}{yes}{no}}
        condition = ${if match_ip{$sender_host_address}{<IP-адрес PT Email Security>}{no}{yes}}
    accept
```

- Сохраните изменения и закройте файл.

4. Добавьте в конфигурацию Exim созданный список контроля доступа:

- Создайте файл `02_exim4-config_acl_pre_options`:

```
sudo nano /etc/exim4/conf.d/main/02_exim4-config_acl_pre_options
```

- Добавьте в файл строку:

```
acl_smtp_connect = acl_check_host
```

- Если вы планируете использовать проверку адресов получателей, включите отправку положительного ответа 250 на команду проверки адреса, добавив в файл строку:

```
acl_smtp_vrfy=accept
```

- Если необходимо изменить максимальный размер письма, добавьте строку:

```
MESSAGE_SIZE_LIMIT = "<Размер в МБ>М"
```

- Сохраните изменения и закройте файл.

5. Настройте получение проверенной почты и уведомлений от PT Email Security:

- Откройте файл `update-exim4.conf.conf`:

```
sudo nano /etc/exim4/update-exim4.conf.conf
```

- Добавьте в файл строку, указав IP-адрес и порт Exim для проверенных писем:

```
dc_local_interfaces='0.0.0.0 ; <IP-адрес Exim>.<Порт Exim>'
```

- Разрешите пересылку уведомлений PT Email Security через Exim, добавив в файл строку с IP-адресом SMTP-сервера PT Email Security:

```
dc_relay_nets='<IP-адрес PT Email Security>'
```

- Сохраните изменения и закройте файл.

6. Сгенерируйте конфигурационный файл Exim:

```
sudo update-exim4.conf
```

7. Перезапустите службу Exim:

```
sudo service exim4 restart
```

Маршрутизация писем через PT Email Security настроена.

13.10. Exim 4 в режиме зеркалирования

При подключении источника скрытые копии писем с сервера Exim отправляются на проверку в PT Email Security. Проверка не влияет на доставку писем получателям.

Внимание! Если в вашей информационной системе используется межсетевой экран или другие средства контроля сетевого трафика, требуется настроить в них правила, разрешающие передачу трафика через порт TCP 25 от почтового сервера к основному узлу PT Email Security.

Для подключения источника к PT Email Security необходимо:

- Добавить в PT Email Security источник с типом **Почтовый сервер в режиме зеркалирования**.
- На сервере Exim настроить отправку скрытых копий писем в PT Email Security.
- Если при обработке писем необходимо использовать адреса электронной почты конечных получателей, настроить на сервере Exim заполнение заголовков писем X-Original-Rcpt-To.

Добавление источника в PT Email Security

► Чтобы добавить источник в PT Email Security:

1. В главном меню выберите **Источники**.
2. Нажмите кнопку **Добавить источник**.
3. В поле **Название** введите название источника, которое будет указано в свойствах полученных от него объектов.

Название должно содержать не менее пяти символов и быть уникальным среди названий всех источников. Название может содержать только строчные буквы латинского алфавита, цифры, дефис и при этом начинаться и заканчиваться только буквами.

4. В раскрывающемся списке **Тип** выберите **Почтовый сервер в режиме зеркалирования**.
5. Если необходимо, в поле **IP-адреса SMTP-сервера** введите дополнительные адреса.
Примечание. В поле указан IP-адрес SMTP-сервера, создаваемого в PT Email Security. Он понадобится вам при настройке источника.
6. Если необходимо, измените стандартный порт подключения к серверу.
Внимание! Указанный порт не должен использоваться другими источниками для проверки, службами или приложениями ОС.
7. Если при подключении используется протокол SSL, установите флажок **Подключаться по SSL**.
Примечание. При снятом флажке передаваемые данные зашифровываются при помощи расширения STARTTLS. Если почтовый сервер организации не поддерживает STARTTLS, данные передаются без шифрования.
8. Если необходимо принимать письма только с определенных адресов, включите фильтрацию входящих подключений и укажите IP-адреса разрешенных узлов или подсетей.
9. Если необходимо, включите использование при обработке писем электронных адресов конечных получателей.
10. Нажмите кнопку **Добавить источник**.

Источник добавлен в PT Email Security.

Настройка источника

На источнике необходимо настроить отправку скрытых копий писем на сервер, созданный при добавлении источника в PT Email Security.

Инструкция разработана для Exim версии 4 с отдельными файлами конфигурации. Если вы используете единый конфигурационный файл, указанные в инструкции строки необходимо добавлять в этот файл. Дополнительную информацию вы можете получить на сайте exim.org.

► Чтобы настроить отправку скрытых копий писем:

1. Создайте файл `03_exim4-config_redirect`:

```
sudo nano /etc/exim4/conf.d/router/03_exim4-config_redirect
```
2. Добавьте в файл строки:

```
bcc:  
driver = redirect
```

```
data = bcc@emailsecurity.local
unseen
```

3. Сохраните изменения и закройте файл.

4. Создайте файл `03_exim4-config_send`:

```
sudo nano /etc/exim4/conf.d/router/03_exim4-config_send
```

5. Добавьте в файл строки, указав IP-адрес и порт PT Email Security для отправки скрытых копий писем:

```
cmdfilter:
    driver = manualroute
    domains = emailsecurity.local
    transport = remote_smtp
    route_list = "* <IP-адрес>:<Порт>"
    self = send
```

6. Сохраните изменения и закройте файл.

7. Перезапустите службу Exim:

```
sudo service exim4 restart
```

Отправка скрытых копий писем настроена.

13.11. Microsoft Exchange 2010—2019 с установленным почтовым агентом

При подключении источника почтовый агент перехватывает все письма, проходящие через сервер Microsoft Exchange, и отправляет их на проверку в PT Email Security, после чего возвращает их обратно для дальнейшей доставки адресатам. В случае потери связи между почтовым агентом и PT Email Security письма доставляются без проверки.

Внимание! Если в вашей информационной системе используется межсетевой экран или другие средства контроля сетевого трафика, требуется настроить в них правила, разрешающие передачу трафика через порт TCP 7536 от основного узла PT Email Security к узлу источника.

Примечание. В схеме обработки писем Microsoft Exchange почтовый агент встраивается на уровне транспортного сервиса в качестве Routing Agent. Используя штатные средства Microsoft Exchange, вы можете отслеживать длину очереди из писем на почтовом агенте.

Почтовый агент может работать со следующими версиями Microsoft Exchange:

- Microsoft Exchange 2010 версии 14;
- Microsoft Exchange 2013 версии 15.0 (кроме 15.0.847.32);
- Microsoft Exchange 2016 версии 15.1;
- Microsoft Exchange 2019 версии 15.2.

Для работы почтового агента на сервере Microsoft Exchange должна быть установлена операционная система Windows Server версии 2012 или выше.

Для подключения источника к PT Email Security необходимо:

- На сервере Microsoft Exchange установить почтовый агент.
- Добавить в PT Email Security источник с типом **Сервер Microsoft Exchange с установленным агентом**.

Установка агента для стандартного сетевого интерфейса

Инструкцию необходимо выполнять на сервере Microsoft Exchange с ролью Mailbox от имени учетной записи с правами администратора операционной системы.

► Чтобы установить почтовый агент:

1. Скопируйте архив с установщиком почтового агента на узел с Microsoft Exchange.
2. Распакуйте архив в любую папку и откройте эту папку.
3. Запустите файл `install.cmd` от имени администратора.

Начнется установка почтового агента.

Почтовый агент установлен.

Установка агента с выбором сетевого интерфейса

Если на узле Microsoft Exchange доступно несколько сетевых интерфейсов или если используется нестандартный порт, то при установке почтового агента необходимо указать, какой интерфейс и порт использовать.

Инструкцию необходимо выполнять на сервере Microsoft Exchange с ролью Mailbox от имени учетной записи с правами администратора операционной системы.

► Чтобы установить почтовый агент:

1. Скопируйте архив с установщиком почтового агента на узел с Microsoft Exchange.
2. Распакуйте архив в любую папку и откройте эту папку.
3. Запустите Windows PowerShell от имени администратора.
4. Запустите установку почтового агента, указав IP-адрес и порт сетевого интерфейса:
`.\install.ps1 -BalancerEndpoint "<IP-адрес>:<Порт>"`

Примечание. Для использования стандартного сетевого интерфейса вы можете ввести IP-адрес 0.0.0.0.

Начнется установка почтового агента.

Почтовый агент установлен.

Удаление почтового агента

Инструкцию необходимо выполнять на сервере Microsoft Exchange с ролью Mailbox от имени учетной записи с правами администратора операционной системы.

► Чтобы удалить почтовый агент:

1. Скопируйте архив с установщиком почтового агента на узел с Microsoft Exchange.
2. Распакуйте архив в любую папку и откройте эту папку.
3. Откройте интерфейс командной строки Windows от имени администратора.
4. Запустите удаление почтового агента:

```
install.cmd -Uninstall
```

Начнется удаление почтового агента. В процессе удаления будет перезапущена служба MS Exchange Transport.

Почтовый агент удален.

Добавление источника в PT Email Security

► Чтобы добавить источник в PT Email Security:

1. В главном меню выберите **Источники**.
2. Нажмите кнопку **Добавить источник**.
3. В поле **Название** введите название источника, которое будет указано в свойствах полученных от него объектов.

Название должно содержать не менее пяти символов и быть уникальным среди названий всех источников. Название может содержать только строчные буквы латинского алфавита, цифры, дефис и при этом начинаться и заканчиваться только буквами.

4. В раскрывающемся списке **Тип** выберите **Сервер Microsoft Exchange с установленным агентом**.
5. В поле **Доменное имя или IP-адрес сервера** введите адрес сервера Microsoft Exchange.
6. Если необходимо, измените стандартный порт подключения к серверу.
7. Нажмите кнопку **Добавить источник**.

Источник добавлен в PT Email Security.

13.12. Microsoft Exchange 2010—2019 в режиме зеркалирования

При подключении источника скрытые копии писем с сервера Microsoft Exchange отправляются на проверку в PT Email Security. Проверка не влияет на доставку писем получателям.

Внимание! Если в вашей информационной системе используется межсетевой экран или другие средства контроля сетевого трафика, требуется настроить в них правила, разрешающие передачу трафика через порт TCP 25 от почтового сервера к основному узлу PT Email Security.

Для подключения источника к PT Email Security необходимо:

- Добавить в PT Email Security источник с типом **Почтовый сервер в режиме зеркалирования**.
- На сервере Microsoft Exchange настроить отправку скрытых копий писем в PT Email Security.
- Если при обработке писем необходимо использовать адреса электронной почты конечных получателей, настроить на сервере Microsoft Exchange заполнение заголовков писем X-Original-Rcpt-To.

Добавление источника в PT Email Security

► Чтобы добавить источник в PT Email Security:

1. В главном меню выберите **Источники**.
2. Нажмите кнопку **Добавить источник**.
3. В поле **Название** введите название источника, которое будет указано в свойствах полученных от него объектов.

Название должно содержать не менее пяти символов и быть уникальным среди названий всех источников. Название может содержать только строчные буквы латинского алфавита, цифры, дефис и при этом начинаться и заканчиваться только буквами.

4. В раскрывающемся списке **Тип** выберите **Почтовый сервер в режиме зеркалирования**.
5. Если необходимо, в поле **IP-адреса SMTP-сервера** введите дополнительные адреса.

Примечание. В поле указан IP-адрес SMTP-сервера, создаваемого в PT Email Security. Он понадобится вам при настройке источника.

6. Если необходимо, измените стандартный порт подключения к серверу.

Внимание! Указанный порт не должен использоваться другими источниками для проверки, службами или приложениями ОС.

7. Если при подключении используется протокол SSL, установите флажок **Подключаться по SSL**.

Примечание. При снятом флажке передаваемые данные зашифровываются при помощи расширения STARTTLS. Если почтовый сервер организации не поддерживает STARTTLS, данные передаются без шифрования.

8. Если необходимо принимать письма только с определенных адресов, включите фильтрацию входящих подключений и укажите IP-адреса разрешенных узлов или подсетей.
9. Если необходимо, включите использование при обработке писем электронных адресов конечных получателей.
10. Нажмите кнопку **Добавить источник**.

Источник добавлен в PT Email Security.

Настройка источника

На источнике необходимо настроить отправку скрытых копий писем на сервер, созданный при добавлении источника в PT Email Security.

Инструкция разработана для сервера Microsoft Exchange версии 2010 и выше. Инструкцию необходимо выполнять от имени учетной записи, которой в центре администрирования Exchange была назначена роль «Управление организацией». Подробную информацию вы можете получить на сайте technet.microsoft.com.

► Чтобы настроить отправку скрытых копий писем в PT Email Security:

1. Запустите центр администрирования Exchange.
2. В главном меню выберите раздел **поток обработки почты**.
Откроется страница **правила**.
3. Нажмите **+** и в раскрывшемся меню выберите **Создать новое правило**.
Откроется окно **новое правило**.
4. В поле **Имя** введите произвольное название правила, например PT Email Security.
5. В раскрывающемся списке **Применить это правило** выберите **Применить ко всем сообщениям**.
6. В раскрывающемся списке **Выполнить следующие действия** выберите **Отправить скрытую копию сообщения (СК)**.
Откроется окно **Выбрать членов**.
7. В поле **добавить** введите `bcc@emailsecurity.local`.
8. Нажмите кнопку **ОК**, затем кнопку **Сохранить**.
9. В панели инструментов нажмите **соединители отправки**.

Откроется страница **соединители**.

10. Нажмите **+**, чтобы добавить соединитель отправки.

Откроется мастер **новый соединитель отправки**.

11. Нажмите кнопку **далее**, оставив значения остальных параметров без изменений.

Откроется следующий шаг мастера.

12. Выберите вариант **Перенаправлять почту через промежуточные узлы**.

13. Нажмите **+**, чтобы добавить промежуточный узел.

Откроется страница **изменить промежуточный узел**.

14. В поле введите IP-адрес bcc-сервера PT Email Security. Если номер TCP-порта для SMTP отличается от стандартного (25), укажите его через двоеточие после IP-адреса.

15. Нажмите кнопку **Сохранить**.

Промежуточный узел будет создан. Откроется следующий шаг мастера.

16. Нажмите **+**, чтобы добавить адресное пространство.

Откроется страница **добавление домена**.

17. В поле **Полное доменное имя (FQDN)** введите `emailsecurity.local`.

18. Нажмите кнопку **Сохранить**, затем кнопку **Далее**, затем кнопку **Готово**.

Информация о новом соединителе отправки появится в таблице **соединители**.

Отправка скрытых копий писем настроена.

13.13. Postfix 3.2 в режиме фильтрации

При подключении источника письма с сервера Postfix отправляются на проверку в PT Email Security, после чего возвращаются обратно для дальнейшей доставки.

Внимание! Если в вашей информационной системе используется межсетевой экран или другие средства контроля сетевого трафика, требуется настроить в них правила, разрешающие передачу трафика через порт TCP 25 от почтового сервера к основному узлу PT Email Security.

Для подключения источника к PT Email Security необходимо:

1. Добавить в PT Email Security источник с типом **Почтовый сервер в режиме фильтрации** или **Почтовый сервер в режиме фильтрации (MTA)**.
2. Настроить в PT Email Security отправку проверенных писем:
 - Если используется несколько почтовых серверов, добавить правила маршрутизации.
 - Если используются непубличные почтовые серверы и требуется TLS-шифрование с проверкой сертификата, добавить корневой сертификат центра сертификации вашей организации.
 - Если на почтовых серверах поддерживается проверка адресов получателей, включить такую проверку для добавленного источника.
3. На сервере Postfix настроить маршрутизацию писем через PT Email Security.

Добавление источника в PT Email Security

► Чтобы добавить источник в PT Email Security:

1. В главном меню выберите **Источники**.
2. Нажмите кнопку **Добавить источник**.
3. В поле **Название** введите название источника, которое будет указано в свойствах полученных от него объектов.

 Название должно содержать не менее пяти символов и быть уникальным среди названий всех источников. Название может содержать только строчные буквы латинского алфавита, цифры, дефис и при этом начинаться и заканчиваться только буквами.
4. В раскрывающемся списке **Тип** выберите:
 - Если для работы с письмами от источника необходимо использовать встроенный в PT Email Security почтовый транспортный агент, выберите **Почтовый сервер в режиме фильтрации (MTA)**.
 - Если в этом нет необходимости, выберите **Почтовый сервер в режиме фильтрации**.
5. Если вы выбрали тип **Почтовый сервер в режиме фильтрации (MTA)**, в блоке параметров **Режим обработки писем** выберите режим:
 - Если хранение и доставку проверенных писем должен контролировать PT Email Security, выберите **Асинхронный**.
 - Если это должен делать почтовый сервер, выберите **Синхронный**.
6. В блоке **Параметры подключения** настройте параметры SMTP-сервера, создаваемого в PT Email Security для приема писем:
 - Если необходимо, в поле **IP-адреса SMTP-сервера** введите дополнительные адреса.

Примечание. В поле указан IP-адрес SMTP-сервера, создаваемого в PT Email Security. Он понадобится вам при настройке источника.

- Если необходимо, измените стандартный порт подключения к серверу.

Внимание! Указанный порт не должен использоваться другими источниками для проверки, службами или приложениями ОС.

- Если при подключении используется протокол SSL, установите флажок **Подключаться по SSL**.

Примечание. При снятом флажке передаваемые данные шифруются при помощи расширения STARTTLS. Если почтовый сервер организации не поддерживает STARTTLS, данные передаются без шифрования.

7. Если необходимо принимать письма только с определенных адресов, включите фильтрацию входящих подключений и укажите IP-адреса разрешенных узлов или подсетей.
8. Если требуется, в блоке параметров **Правила маршрутизации почтового трафика** в раскрывающемся списке **Доверенные сертификаты TLS-шифрования** выберите для всех правил маршрутизации, какой набор доверенных сертификатов будет использоваться для проверки сертификатов почтовых серверов:
 - Если только доверенные сертификаты из внутреннего хранилища PT Email Security, выберите **Пользовательские**.
 - Если сертификаты из внутреннего хранилища и глобальные сертификаты, доступные внутри докер-контейнеров PT Email Security, выберите **Глобальные и пользовательские**.
9. Добавьте правило маршрутизации по умолчанию и укажите в нем параметры сервера для отправки писем и уведомлений о результатах проверки:
 - Нажмите кнопку **Добавить**.
 - В блоке параметров **Требования к TLS-шифрованию** укажите для всех почтовых серверов в правиле, требуется ли TLS-шифрование.
 - Если при шифровании требуется проверять сертификат почтового сервера, установите флажок **Проверять сертификат**.
 - В поле **Доменное имя или IP-адрес** введите адрес и порт сервера.
 - Если в вашей организации используется несколько почтовых серверов, в поле **Приоритет** введите число, соответствующее приоритету сервера с указанным адресом.

Примечание. Вы можете указать число от 1 до 65535. Чем меньше число, тем выше приоритет сервера. Письма будут отправляться на активные серверы с наибольшим приоритетом. Если для серверов указан одинаковый приоритет, почтовый трафик балансируется между ними поровну.

- В раскрывающемся списке **Режим запуска TLS-шифрования** выберите режим запуска шифрования для этого сервера.
- Если для доступа к серверу требуется аутентификация, включите использование аутентификации и в раскрывающемся списке **Тип аутентификации** выберите ее тип.

Примечание. При автоматическом выборе типа аутентификации PT Email Security выбирает наиболее безопасный тип из предложенных почтовым сервером.

- Если используется аутентификация, в поля **Логин** и **Пароль** введите учетные данные для доступа к серверу.
- Если в вашей организации используется несколько почтовых серверов, по кнопке **Добавить сервер** добавьте для них блоки параметров и настройте аналогичным образом.
- Нажмите кнопку **Добавить**.

10. Нажмите кнопку **Добавить источник**.

Источник добавлен в PT Email Security.

Добавление правила маршрутизации проверенных писем в PT Email Security

Если необходимо использовать различные почтовые серверы в зависимости от домена в адресе электронной почты получателя, вы можете настроить в PT Email Security [правила маршрутизации проверенных писем](#) (см. раздел 12.2).

► Чтобы добавить правило маршрутизации:

1. В главном меню выберите **Источники**.
2. В панели с информацией об источнике перейдите по ссылке **Параметры источника**.
3. В блоке параметров **Правила маршрутизации почтового трафика** нажмите кнопку **Добавить**.
4. В поле **Домен электронной почты получателя** введите доменную часть адреса электронной почты получателей, для которых необходимо настроить правило.

С помощью звездочки вы можете задать маску для доменной части адреса получателей писем, если доменная часть содержит поддомены третьего уровня или выше. Например, правило с маской *.example.com будет применяться и для адресов с доменной частью example.com, sub_1.example.com, sub_2.example.com, и для адресов с доменной частью, содержащей поддомены более высоких уровней.

Примечание. Если доменная часть адреса получателя соответствует нескольким правилам маршрутизации, будет использовано то правило, в котором указан наиболее точный адрес. При этом более высокий приоритет имеют правила, в которых не используются маски.

5. В блоке параметров **Требования к TLS-шифрованию** укажите для всех почтовых серверов в правиле, требуется ли TLS-шифрование.
6. Если при шифровании требуется проверять сертификат почтового сервера, установите флажок **Проверять сертификат**.
7. Если необходимо перенаправлять письма согласно MX-записям, выберите способ маршрутизации **По MX-записям**.

Внимание! Письмо не будет отправлено, если в DNS отсутствует подходящая MX- или A-запись для указанного домена.

8. Если необходимо перенаправлять письма на определенный почтовый сервер, выберите способ маршрутизации **По адресам почтовых серверов** и укажите параметры сервера:

- В поле **Доменное имя или IP-адрес** введите адрес и порт сервера.
- Если в вашей организации используется несколько почтовых серверов, в поле **Приоритет** введите число, соответствующее приоритету сервера с указанным адресом.

Примечание. Вы можете указать число от 1 до 65535. Чем меньше число, тем выше приоритет сервера. Письма будут отправляться на активные серверы с наибольшим приоритетом. Если для серверов указан одинаковый приоритет, почтовый трафик балансируется между ними поровну.

- В раскрывающемся списке **Режим запуска TLS-шифрования** выберите режим запуска шифрования для этого сервера.
- Если для доступа к серверу требуется аутентификация, включите использование аутентификации и в раскрывающемся списке **Тип аутентификации** выберите ее тип.

Примечание. При автоматическом выборе типа аутентификации PT Email Security выбирает наиболее безопасный тип из предложенных почтовым сервером.

- Если используется аутентификация, в поля **Логин** и **Пароль** введите учетные данные для доступа к серверу.
- Если в вашей организации используется несколько почтовых серверов, по кнопке **Добавить сервер** добавьте для них блоки параметров и настройте аналогичным образом.

9. Нажмите кнопку **Добавить**.

10. Нажмите кнопку **Сохранить**.

Правило маршрутизации добавлено.

Добавление доверенных сертификатов в PT Email Security

Если при отправке проверенных писем вы планируете использовать TLS-шифрование с проверкой сертификата, при проверке сертификатов почтовых серверов будут использоваться следующие сертификаты:

- Для публичных SMTP-серверов — сертификаты доверенных центров сертификации, доступные внутри докер-контейнеров PT Email Security.
- Для непубличных SMTP-серверов вашей организации — доверенные сертификаты центров сертификации вашей организации. Корневые сертификаты этих центров необходимо добавить в PT Email Security.

Инструкции необходимо выполнять на основном узле PT Email Security. Поддерживаются только сертификаты формата PEM.

- ▶ Чтобы добавить сертификат в PT Email Security,

выполните команду:

```
sudo ptmsctl system trusted-certs add --name <Название сертификата> --path <Полный путь к файлу сертификата>
```

Например:

```
sudo ptmsctl system trusted-certs add --name example_cert --path /etc/tls/certs/rootCA.crt
```

- ▶ Чтобы просмотреть список добавленных в PT Email Security сертификатов,

выполните команду:

```
sudo ptmsctl system trusted-certs list
```

Примечание. Вы можете просмотреть информацию об отдельном сертификате, выполнив команду `sudo ptmsctl system trusted-certs view --name <Название сертификата>`.

- ▶ Чтобы удалить сертификат из PT Email Security,

выполните команду:

```
sudo ptmsctl system trusted-certs delete --name <Название сертификата>
```

Например:

```
sudo ptmsctl system trusted-certs delete --name example_cert
```

Включение проверки адресов получателей

Перед отправкой проверенных писем PT Email Security может проверять адреса получателей на принимающих почтовых серверах с помощью SMTP-команды `VERFY` (согласно спецификации RFC 5321). По умолчанию эта проверка отключена, поскольку на некоторых почтовых серверах выполнение этой команды может быть заблокировано по соображениям безопасности. Вы можете включить для источника проверку адресов получателей, если для него добавлено хотя бы одно правило маршрутизации или указано более одного почтового сервера. Инструкцию необходимо выполнить на основном узле PT Email Security.

- ▶ Чтобы включить проверку адресов получателей для источника,

выполните команду:

```
sudo ptmsctl system components config patch --component <Название источника> --toml "[smtp_client_config.verify_recipients]
enabled = true
"
```

Настройка источника

На сервере Postfix необходимо настроить маршрутизацию писем через PT Email Security.

- ▶ Чтобы настроить маршрутизацию писем через PT Email Security:

1. Откройте файл `/etc/postfix/main.cf`:
`sudo nano /etc/postfix/main.cf`
2. Добавьте в файл строки, указав IP-адрес и порт SMTP-сервера PT Email Security:
`content_filter=scan:[<IP-адрес PT Email Security>]:<Порт PT Email Security>`
`receive_override_options=no_address_mappings`
3. Сохраните изменения и закройте файл.
4. Откройте файл `/etc/postfix/master.cf`:
`sudo nano /etc/postfix/master.cf`
5. Добавьте в файл строки, указав IP-адрес и порт сервера Postfix для проверенных писем и IP-адрес SMTP-сервера PT Email Security:

```
scan unix - - n - 10 smtp
-o disable_dns_lookups=yes
-o smtp_data_done_timeout=1200
-o disable_mime_output_conversion=yes
-o max_use=8
<IP-адрес Postfix>:<Порт Postfix> inet n - n - 10 smtpd
-o mynetworks=<IP-адрес PT Email Security>
-o smtpd_client_restrictions=permit_mynetworks,reject
-o smtpd_helo_restrictions=
-o smtpd_sender_restrictions=
-o content_filter=
-o receive_override_options=no_unknown_recipient_checks,no_header_body_checks,no_milters
```

Примечание. Для проверки адресов получателей должна быть включена отправка положительного ответа 250 на команду проверки адреса, для параметра `disable_vrfy_command` должно быть указано значение `no`.

6. Сохраните изменения и закройте файл.
7. Перезапустите службу сервера Postfix:
`service postfix restart`

Маршрутизация писем через PT Email Security настроена.

13.14. Postfix 3.2 в режиме зеркалирования

При подключении источника скрытые копии писем с сервера Postfix отправляются на проверку в PT Email Security. Проверка не влияет на доставку писем получателям.

Внимание! Если в вашей информационной системе используется межсетевой экран или другие средства контроля сетевого трафика, требуется настроить в них правила, разрешающие передачу трафика через порт TCP 25 от почтового сервера к основному узлу PT Email Security.

Для подключения источника к PT Email Security необходимо:

- Добавить в PT Email Security источник с типом **Почтовый сервер в режиме зеркалирования**.
- На сервере Postfix настроить отправку скрытых копий писем в PT Email Security.
- Если при обработке писем необходимо использовать адреса электронной почты конечных получателей, настроить на сервере Postfix заполнение заголовков писем X-Original-Rcpt-To.

Добавление источника в PT Email Security

► Чтобы добавить источник в PT Email Security:

1. В главном меню выберите **Источники**.
2. Нажмите кнопку **Добавить источник**.
3. В поле **Название** введите название источника, которое будет указано в свойствах полученных от него объектов.

Название должно содержать не менее пяти символов и быть уникальным среди названий всех источников. Название может содержать только строчные буквы латинского алфавита, цифры, дефис и при этом начинаться и заканчиваться только буквами.

4. В раскрывающемся списке **Тип** выберите **Почтовый сервер в режиме зеркалирования**.
5. Если необходимо, в поле **IP-адреса SMTP-сервера** введите дополнительные адреса.

Примечание. В поле указан IP-адрес SMTP-сервера, создаваемого в PT Email Security. Он понадобится вам при настройке источника.

6. Если необходимо, измените стандартный порт подключения к серверу.

Внимание! Указанный порт не должен использоваться другими источниками для проверки, службами или приложениями ОС.

7. Если при подключении используется протокол SSL, установите флажок **Подключаться по SSL**.

Примечание. При снятом флажке передаваемые данные зашифровываются при помощи расширения STARTTLS. Если почтовый сервер организации не поддерживает STARTTLS, данные передаются без шифрования.

8. Если необходимо принимать письма только с определенных адресов, включите фильтрацию входящих подключений и укажите IP-адреса разрешенных узлов или подсетей.
9. Если необходимо, включите использование при обработке писем электронных адресов конечных получателей.
10. Нажмите кнопку **Добавить источник**.

Источник добавлен в PT Email Security.

Настройка источника

На сервере Postfix необходимо настроить отправку скрытых копий писем на сервер, созданный при добавлении источника в PT Email Security.

► Чтобы настроить отправку скрытых копий писем:

1. Создайте карту `transport` с описанием транспорта для отправки скрытых копий писем в PT Email Security:
 - Создайте файл `/etc/postfix/maps/transport`.
 - Добавьте в файл строку и укажите в ней IP-адрес и порт PT Email Security:
`bcc@emailsecurity.local smtp-bcc:[<IP-адрес>]:<Порт>`
 - Сохраните изменения и закройте файл.
2. Добавьте карту `transport` в конфигурацию сервера:
 - Откройте файл `/etc/postfix/main.cf`.
 - Добавьте в файл строки:
`always_bcc = bcc@emailsecurity.local`
`transport_maps = hash:/etc/postfix/maps/transport`
 - Сохраните изменения и закройте файл.
3. Обновите файл соответствий:
`sudo postmap /etc/postfix/maps/transport`
4. Добавьте транспорт `smtp-bcc` в конфигурацию сервера:
 - Откройте файл `/etc/postfix/master.cf`.
 - Добавьте в файл строку:
`smtp-bcc unix - - y - - smtp`

- Сохраните изменения и закройте файл.

5. Перезапустите службу сервера Postfix:

```
sudo systemctl restart postfix
```

Отправка скрытых копий писем настроена.

Настройка заполнения заголовка X-Original-Rcpt-To

Если при обработке писем в PT Email Security планируется использовать электронные адреса конечных получателей, на сервере Postfix необходимо настроить заполнение заголовков писем X-Original-Rcpt-To.

► Чтобы настроить заполнение в письмах заголовка X-Original-Rcpt-To:

1. Создайте карту `detect_recipients` для добавления заголовка X-Original-Rcpt-To во все письма:

- Создайте файл `/etc/postfix/maps/detect_recipients`.

- Добавьте в файл строку:

```
/^(.+)$/ PREPEND X-Original-Rcpt-To: $1
```

- Сохраните изменения и закройте файл.

2. Добавьте карту `detect_recipients` в параметры обработки команды RCPT TO:

- Откройте файл `/etc/postfix/main.cf`.

- Добавьте в файл строку для параметра `smtpd_recipient_restrictions`:

```
smtpd_recipient_restrictions =  
    ...  
    check_recipient_access regexp:/etc/postfix/maps/detect_recipients
```

- Сохраните изменения и закройте файл.

3. Создайте карту `header_checks` для удаления заголовка X-Original-Rcpt-To из писем конечным получателям:

- Создайте файл `/etc/postfix/maps/header_checks`.

- Добавьте в файл строку:

```
/^X-Original-Rcpt-To:/ IGNORE
```

- Сохраните изменения и закройте файл.

4. Укажите карту `header_checks` в параметрах обработки заголовков писем для используемых транспортов:

- Откройте файл `/etc/postfix/master.cf`.

- Если используется транспорт `smtp` (для пересылки писем на другие серверы), добавьте в файл строку для этого транспорта:

```
smtp unix - - y - - smtp  
    -o smtp_header_checks=regexp:/etc/postfix/maps/header_checks
```

- Если используется транспорт lmtp (для локальной доставки писем), добавьте в файл строку для этого транспорта:

```
lmtp unix - - y - - lmtp
    -o lmtp_header_checks=regex:/etc/postfix/maps/header_checks
```

- Сохраните изменения и закройте файл.

5. Перезапустите службу сервера Postfix:

```
sudo systemctl restart postfix
```

Заполнение заголовка X-Original-Rcpt-To настроено.

13.15. PT Threat Analyzer 2.10 и выше

При подключении источника копии объектов из PT Threat Analyzer отправляются на проверку в PT Email Security через публичный API.

Внимание! Если в вашей информационной системе используется межсетевой экран или другие средства контроля сетевого трафика, требуется настроить в них правила, разрешающие передачу трафика через порты TCP 80, 443 от узла источника к основному узлу PT Email Security.

Для подключения источника в PT Email Security необходимо:

- Выпустить токен доступа к публичному API с разрешенным действием **Проверка с параметрами источника**.
- Добавить в PT Email Security источник с типом **API с выбранными параметрами проверки**.

Для подключения источника в PT Threat Analyzer необходимо настроить отправку объектов в PT Email Security.

Добавление источника в PT Email Security

► Чтобы добавить источник в PT Email Security:

1. В главном меню выберите **Источники**.
2. Нажмите кнопку **Добавить источник**.
3. В поле **Название** введите название источника, которое будет указано в свойствах полученных от него объектов.

Название должно содержать не менее пяти символов и быть уникальным среди названий всех источников. Название может содержать только строчные буквы латинского алфавита, цифры, дефис и при этом начинаться и заканчиваться только буквами.

4. В раскрывающемся списке **Тип** выберите **API с выбранными параметрами проверки**.

5. В раскрывающемся списке **Токен доступа** выберите токен доступа к публичному API.
6. Нажмите кнопку **Добавить источник**.

Источник добавлен в PT Email Security.

Настройка источника

На узле PT Threat Analyzer необходимо настроить отправку объектов на проверку в PT Email Security через публичный API.

► Чтобы настроить отправку объектов в PT Email Security:

1. Откройте конфигурационный файл `threat-analyzer-installer-<Версия>/group_vars/all/configuration.yml`.
2. В параметре `cybsi_pt_sb_host` укажите IP-адрес (доменное имя) основного узла PT Email Security.
3. В параметре `cybsi_pt_sb_api_key` укажите токен доступа к публичному API PT Email Security.
4. Сохраните изменения и закройте файл.

Отправка объектов в PT Email Security настроена.

13.16. Squid 3 и выше

При подключении источника объекты с прокси-сервера Squid отправляются на проверку в PT Email Security по протоколу ICAP. В зависимости от приобретенной вами лицензии и выбранных параметров работы ICAP-сервера PT Email Security проверка может выполняться в режиме ожидания, в пассивном или блокирующем режиме.

Внимание! Если в вашей информационной системе используется межсетевой экран или другие средства контроля сетевого трафика, требуется настроить в них правила, разрешающие передачу трафика через порт TCP 1344 от узла источника к основному узлу PT Email Security.

Для подключения источника к PT Email Security необходимо:

- Добавить в PT Email Security источник с типом **ICAP-сервер**.
- На прокси-сервере Squid настроить ICAP-клиент для работы с ICAP-сервером PT Email Security.

Добавление источника в PT Email Security

► Чтобы добавить источник в PT Email Security:

1. В главном меню выберите **Источники**.
2. Нажмите кнопку **Добавить источник**.

3. В поле **Название** введите название источника, которое будет указано в свойствах полученных от него объектов.

Название должно содержать не менее пяти символов и быть уникальным среди названий всех источников. Название может содержать только строчные буквы латинского алфавита, цифры, дефис и при этом начинаться и заканчиваться только буквами.

4. В раскрывающемся списке **Тип** выберите **ICAP-сервер**.
5. Если необходимо, в поле **IP-адреса ICAP-сервера** введите дополнительные адреса.

Примечание. В поле указан IP-адрес ICAP-сервера, создаваемого в PT Email Security. Он понадобится вам при настройке источника.

6. Если необходимо, измените стандартный порт подключения к ICAP-серверу.

Внимание! Указанный порт не должен использоваться другими источниками для проверки, службами или приложениями ОС.

7. Если необходимо принимать объекты только с определенных адресов, включите фильтрацию входящих подключений и укажите IP-адреса разрешенных узлов или подсетей.
8. Нажмите кнопку **Добавить источник**.

Источник добавлен в PT Email Security.

Настройка источника

На узле прокси-сервера Squid необходимо настроить ICAP-клиент для работы с ICAP-сервером, созданным при добавлении источника в PT Email Security.

Внимание! Инструкция не содержит описания настройки аутентификации пользователей. Более подробную информацию о настройке Squid вы можете получить на сайте squid-cache.org.

При настройке ICAP-клиента вам необходимо указать ссылку для обращения к ICAP-серверу PT Email Security. Вид ссылки зависит от режима проверки объектов и режима работы ICAP-сервера:

- Ссылки для проверки объектов в блокирующем режиме:
 - REQMOD: `icap://<IP-адрес>:<Порт>/scanrequest?modify=y&block-unwanted=<Блокировать потенциально опасные>&timeout=<Тайм-аут>`
 - RESPMOD: `icap://<IP-адрес>:<Порт>/scanresponse?modify=y&block-unwanted=<Блокировать потенциально опасные>&timeout=<Тайм-аут>`

Примечание. В параметре `block-unwanted` вы можете указать `y`, если необходимо блокировать потенциально опасные файлы, или `n` — если блокировать такие файлы не требуется (по умолчанию потенциально опасные файлы не блокируются). В параметре `timeout` вы можете указать тайм-аут ответа ICAP-сервера в секундах (по умолчанию 30 секунд).

— Ссылки для проверки объектов в режиме ожидания:

- REQMOD: `icap://<IP-адрес>:<Порт>/scanrequest?modify=no&timeout=<Тайм-аут>`
- RESPMOD: `icap://<IP-адрес>:<Порт>/scanresponse?modify=no&timeout=<Тайм-аут>`

— Ссылки для проверки объектов в пассивном режиме:

- REQMOD: `icap://<IP-адрес>:<Порт>/bypass`
- RESPMOD: `icap://<IP-адрес>:<Порт>/bypass`

► Чтобы настроить ICAP-клиент:

1. Создайте резервную копию конфигурационного файла `/etc/squid3/squid.conf`.

Примечание. Конфигурационный файл Squid также может располагаться в каталоге `/etc/squid/squid.conf` или `/usr/local/squid/etc/squid.conf`.

2. Откройте файл `/etc/squid3/squid.conf`:

```
sudo nano /etc/squid3/squid.conf
```

3. Добавьте в файл строку для включения модуля ICAP:

```
icap_enable on
```

4. Добавьте в файл строку для создания ICAP-службы Squid и укажите для нее ссылку на ICAP-сервер PT Email Security:

- Если используется режим REQMOD:

```
icap_service <Название ICAP-службы> reqmod_precache <Ссылка на ICAP-сервер для REQMOD>
```

- Если используется режим RESPMOD:

```
icap_service <Название ICAP-службы> respmod_precache <Ссылка на ICAP-сервер для RESPMOD>
```

5. Если необходимо, укажите в той же строке дополнительные параметры ICAP-службы, разделяя их пробелами:

- Если необходимо пересылать HTTP-клиенту сообщения, которые не были обработаны из-за ошибок или недоступности ICAP-сервера, добавьте параметр `bypass=1`. По умолчанию Squid передает HTTP-клиенту страницу с сообщением об ошибке.

- Если необходимо переопределить максимальное число одновременных соединений с ICAP-сервером, добавьте параметра `max-conn=<Число соединений>`. По умолчанию установлено 128 соединений.

- Если необходимо настроить поведение в случае превышения максимального числа соединений, добавьте параметр `on-overload=<Действие>`. Доступны следующие действия: `block` — отправить HTTP-клиенту страницу с сообщением об ошибке; `bypass`

— игнорировать ICAP-службу (по умолчанию); `wait` — ожидать освобождения ICAP-соединения; `force` — игнорировать установленное максимальное число одновременных соединений.

6. Добавьте в файл строку для настройки доступа к созданной ICAP-службе:

```
adaptation_access <Название ICAP-службы> <Параметры доступа>
```

Например:

```
adaptation_access ptes_req allow all
adaptation_access ptes_resp allow all
```

7. Если требуется отправлять поле заголовка X-Client-IP с IP-адресом пользователя, скачавшего файл, добавьте в файл строку:

```
adaptation_send_client_ip on
```

8. Если требуется отправлять поле заголовка X-Client-Username с именем пользователя, скачавшего файл, добавьте в файл строки:

```
adaptation_send_username on
icap_client_username_header X-Client-Username
```

9. Сохраните изменения и закройте файл.

10. Перезапустите прокси-сервер Squid:

```
sudo service squid3 reload
```

Примечание. Для перезапуска прокси-сервера Squid также может использоваться команда `sudo service squid reload`.

ICAP-клиент настроен.

13.17. UserGate NGFW 6, 7.1, 7.4

При подключении источника объекты от межсетевого экрана UserGate отправляются на проверку в PT Email Security по протоколу ICAP. В зависимости от приобретенной вами лицензии и выбранных параметров работы ICAP-сервера PT Email Security проверка может выполняться в режиме ожидания, в пассивном или блокирующем режиме.

Внимание! Если в вашей информационной системе используется межсетевой экран или другие средства контроля сетевого трафика, требуется настроить в них правила, разрешающие передачу трафика через порт TCP 1344 от узла источника к основному узлу PT Email Security.

Для подключения источника к PT Email Security необходимо:

- Добавить в PT Email Security источник с типом **ICAP-сервер**.
- На межсетевом экране UserGate настроить ICAP-клиент для работы с ICAP-сервером PT Email Security.

Добавление источника в PT Email Security

► Чтобы добавить источник в PT Email Security:

1. В главном меню выберите **Источники**.
2. Нажмите кнопку **Добавить источник**.
3. В поле **Название** введите название источника, которое будет указано в свойствах полученных от него объектов.

Название должно содержать не менее пяти символов и быть уникальным среди названий всех источников. Название может содержать только строчные буквы латинского алфавита, цифры, дефис и при этом начинаться и заканчиваться только буквами.

4. В раскрывающемся списке **Тип** выберите **ICAP-сервер**.
5. Если необходимо, в поле **IP-адреса ICAP-сервера** введите дополнительные адреса.

Примечание. В поле указан IP-адрес ICAP-сервера, создаваемого в PT Email Security. Он понадобится вам при настройке источника.

6. Если необходимо, измените стандартный порт подключения к ICAP-серверу.

Внимание! Указанный порт не должен использоваться другими источниками для проверки, службами или приложениями ОС.

7. Если необходимо принимать объекты только с определенных адресов, включите фильтрацию входящих подключений и укажите IP-адреса разрешенных узлов или подсетей.
8. Нажмите кнопку **Добавить источник**.

Источник добавлен в PT Email Security.

Настройка источника

Для межсетевого экрана UserGate необходимо настроить ICAP-клиент для работы с ICAP-сервером, созданным при добавлении источника в PT Email Security. Дополнительную информацию о настройке UserGate вы можете получить на сайте usergate.com.

Если UserGate у вас работает в качестве сетевого моста, для работы ICAP-клиента необходимо использовать режим моста Layer 3.

При настройке ICAP-клиента вам необходимо указать ссылку для обращения к ICAP-серверу PT Email Security. Вид ссылки зависит от режима проверки объектов и режима работы ICAP-сервера:

- Ссылки для проверки объектов в блокирующем режиме:
 - REQMOD: /scanrequest?modify=y&block-unwanted=<Блокировать потенциально опасные>&timeout=5
 - RESPMOD: /scanresponse?modify=y&block-unwanted=<Блокировать потенциально опасные>&timeout=5

Примечание. В параметре block-unwanted вы можете указать y, если необходимо блокировать потенциально опасные файлы, или n — если блокировать такие файлы не требуется (по умолчанию потенциально опасные файлы не блокируются). В параметре timeout вы можете изменить тайм-аут ответа ICAP-сервера в секундах.

- Ссылки для проверки объектов в режиме ожидания:
 - REQMOD: /scanrequest?modify=no&timeout=5
 - RESPMOD: /scanresponse?modify=no&timeout=5
- Ссылки для проверки объектов в пассивном режиме:
 - REQMOD: /bypass
 - RESPMOD: /bypass

► Чтобы настроить ICAP-клиент:

1. Откройте браузер и в адресной строке введите IP-адрес веб-интерфейса UserGate.
Откроется веб-консоль UserGate.
2. Авторизуйтесь под учетной записью администратора UserGate.
3. В главном меню перейдите по ссылке **Настройки**.
4. В левой части страницы выберите раздел **Политики безопасности** → **ICAP-серверы**.
5. В панели инструментов нажмите кнопку **Добавить**.
Откроется окно **Свойства ICAP-сервера**.
6. На вкладке **Общие** настройте параметры:
 - В поле **Название** введите название ICAP-сервера.
 - В поле **Адрес сервера** введите адрес ICAP-сервера PT Email Security.
 - Если используемый порт отличается от 1344, в поле **Порт** введите номер порта.
 - Если необходимо изменить максимальный размер отправляемых на проверку файлов, в поле **Максимальный размер сообщения** укажите этот размер (размер по умолчанию — 512 КБ).

Внимание! Увеличение максимального размера отправляемых на проверку файлов приведет к увеличению объема используемой UserGate оперативной памяти. Объем используемой памяти вы можете отслеживать на дашборде **НОС** на виджете **Графики производительности**.

7. Выберите вкладку **Данные** и настройте параметры:

- В строке **Reqmod путь** установите флажок **Включено**, а в поле ниже введите ссылку на ICAP-сервер PT Email Security для REQMOD.

Примечание. Если вы увеличили максимальный размер отправляемых на проверку файлов, необходимо увеличить время проверки каждого файла в PT Email Security, указанное в параметре `timeout`.

- В строке **Respmoд путь** установите флажок **Включено**, а в поле ниже введите ссылку на ICAP-сервер PT Email Security для RESPMOD.

Внимание! Если вы увеличили время проверки файлов в PT Email Security, необходимо также увеличить тайм-аут ответа ICAP-сервера, оно должно быть на 5 секунд больше значения параметра `timeout`. Увеличение тайм-аута ответа ICAP-сервера приведет к увеличению объема используемой UserGate оперативной памяти.

Примечание. По умолчанию тайм-аут ответа ICAP-сервера составляет 10 секунд. Текущее значение тайм-аута вы можете узнать, выполнив на узле UserGate через интерфейс командной строки команду `proxu config -get icap_wait_timeout`. Изменить тайм-аут вы можете командой `proxu config -set icap_wait_timeout <Тайм-аут ответа ICAP-сервера>`.

- В строке **Посылать имя пользователя** установите флажки **Включено** и **Кодировать в base64**, а в поле ниже введите `X-Authenticated-User`.
- В строке **Посылать IP-адрес** установите флажок **Включено**, а в поле ниже введите `X-Client-Ip`.

8. Нажмите кнопку **Сохранить**.

9. В левой части страницы выберите раздел **Политики безопасности** → **ICAP-правила**.

10. В панели инструментов нажмите кнопку **Добавить**.

Откроется окно **Свойства правила ICAP**.

11. На вкладке **Общие** настройте параметры:

- В поле **Название** введите название правила.
- В строке **Действие** по ссылке **Пропустить** откройте раскрывающийся список и выберите **Переслать**.

12. Выберите вкладку **ICAP-серверы**.

13. Нажмите кнопку **Добавить**.

Откроется окно **Выбор ICAP-сервера**.

14. Выберите в списке добавленный ранее ICAP-сервер и нажмите кнопку **Добавить**.

15. Нажмите кнопку **Заккрыть**.

ICAP-клиент настроен.

14. Интеграция с внешними системами

В разделе описаны возможности интеграции PT Email Security с внешними системами.

В этом разделе

[MaxPatrol EDR 6.0 и выше \(см. раздел 14.1\)](#)

[MaxPatrol SIEM 6.1 и выше \(см. раздел 14.2\)](#)

[PT AF 3, 4.2.1 и выше \(см. раздел 14.3\)](#)

[PT ISIM 5.2 и выше \(см. раздел 14.4\)](#)

[PT NAD 7.1 и выше \(см. раздел 14.5\)](#)

[PT NGFW 1.8 и выше \(см. раздел 14.6\)](#)

[PT Threat Analyzer 2.10 и выше \(см. раздел 14.7\)](#)

14.1. MaxPatrol EDR 6.0 и выше

При интеграции продуктов пользователь MaxPatrol EDR с помощью агента на конечном устройстве может отправлять файлы на проверку в PT Email Security. Информация о проверенных файлах заносится в базы данных на агенте и на сервере MaxPatrol EDR. Получить эту информацию можно с помощью SQL-запроса.

Внимание! Если в вашей информационной системе используется межсетевой экран или другие средства контроля сетевого трафика, требуется настроить в них правила, разрешающие передачу трафика через порты TCP 80, 443 от узла с сервером MaxPatrol EDR к основному узлу PT Email Security.

Интеграция осуществляется через публичный API PT Email Security. Для интеграции в MaxPatrol EDR используется модуль «Проверка файлов в PT Email Security».

Примечание. Инструкции по настройке MaxPatrol EDR приведены [в технической документации продукта](#).

Если вы настраиваете интеграцию с MaxPatrol EDR версии 8.0.1 и выше и при этом вы планируете настраивать параметры проверки через веб-интерфейс PT Email Security, вам необходимо:

- В PT Email Security выпустить токен доступа к публичному API с разрешенным действием **Проверка с параметрами источника**.
- Добавить в PT Email Security источник с типом **MaxPatrol EDR**.
- В MaxPatrol EDR настроить модуль «Проверка файлов в PT Email Security» (требуется модуль версии 2.0.0).

Внимание! При настройке модуля необходимо установить флажок **MaxPatrol EDR подключен как источник**.

Если вы настраиваете интеграцию с MaxPatrol EDR версии 8.0.1 и выше и при этом параметры проверки будут передаваться в запросе, вам необходимо:

- В PT Email Security выпустить токен доступа к публичному API с разрешенным действием **Проверка с передаваемыми параметрами**.
- В MaxPatrol EDR настроить модуль «Проверка файлов в PT Email Security» (требуется модуль версии 2.0.0).

Примечание. При настройке модуля флажок о подключении MaxPatrol EDR в качестве источника устанавливать не нужно.

Если вы настраиваете интеграцию с MaxPatrol EDR версий 6.0—8.0.0, вам необходимо:

- В PT Email Security выпустить токен доступа к публичному API с разрешенным действием **Проверка с передаваемыми параметрами**.
- В MaxPatrol EDR настроить модуль «Проверка файлов в PT Email Security».

Добавление источника в PT Email Security

► Чтобы добавить источник в PT Email Security:

1. В главном меню выберите **Источники**.
2. Нажмите кнопку **Добавить источник**.
3. В поле **Название** введите название источника, которое будет указано в свойствах полученных от него объектов.

Название должно содержать не менее пяти символов и быть уникальным среди названий всех источников. Название может содержать только строчные буквы латинского алфавита, цифры, дефис и при этом начинаться и заканчиваться только буквами.

4. В раскрывающемся списке **Тип** выберите **MaxPatrol EDR**.
5. В раскрывающемся списке **Токен доступа** выберите токен доступа к публичному API.
6. Нажмите кнопку **Добавить источник**.

Источник добавлен в PT Email Security.

14.2. MaxPatrol SIEM 6.1 и выше

При интеграции PT Email Security формирует сообщения в формате syslog и отправляет их на внешний syslog-сервер, в качестве которого выступает MaxPatrol SIEM. Например, формируются сообщения о начале и завершении работы с источником, о регистрации нового объекта, о результатах проверок объектов средствами проверки и о вынесении вердиктов по объектам и заданиям. Подробная информация о сообщениях приведена в Руководстве разработчика. На основании полученных сообщений в MaxPatrol SIEM могут регистрироваться события ИБ.

Внимание! Если в вашей информационной системе используется межсетевой экран или другие средства контроля сетевого трафика, необходимо настроить в них правила, разрешающие передачу трафика через порт UDP 514 или TCP 1468 от основного узла PT Email Security к узлу MaxPatrol SIEM.

Примечание. Инструкции по настройке MaxPatrol SIEM приведены [в технической документации продукта](#).

Для настройки интеграции необходимо:

- В MaxPatrol SIEM создать и запустить задачу на сбор событий с профилем **SysLog**.
- В PT Email Security настроить отправку сообщений по протоколу syslog на внешний syslog-сервер.

Настройка PT Email Security для отправки сообщений syslog

► Чтобы настроить отправку сообщений по протоколу syslog на внешний syslog-сервер:

1. В главном меню выберите **Система** → **Основные параметры**.
2. В блоке параметров **Отправка сообщений по протоколу syslog** включите отправку сообщений.
3. В полях **Доменное имя или IP-адрес syslog-сервера** введите адрес и порт внешнего syslog-сервера.
4. Выберите транспортный протокол **TCP** или **UDP**.
5. Если требуется, отключите отправку событий аудита PT Email Security.
6. Нажмите кнопку **Сохранить**.

Изменения будут применены через несколько минут.

Отправка сообщений по протоколу syslog на внешний syslog-сервер настроена.

14.3. PT AF 3, 4.2.1 и выше

При интеграции продуктов PT AF отправляет извлеченные из трафика файлы на проверку в PT Email Security и в случае обнаружения угрозы получает результаты проверки.

Внимание! Если в вашей информационной системе используется межсетевой экран или другие средства контроля сетевого трафика, требуется настроить в них правила, разрешающие передачу трафика через порт TCP 1344 от узла PT AF к основному узлу PT Email Security.

Интеграция осуществляется по ICAP. При этом PT Email Security является ICAP-сервером, а PT AF — ICAP-клиентом, который отправляет извлеченные из трафика файлы на проверку и получает результаты проверки. В PT Email Security также отправляется дополнительная информация о файлах, например протокол, по которому перехвачен файл, и IP-адреса узлов, между которыми он передавался.

Примечание. Инструкции по настройке PT AF приведены [в технической документации продукта](#).

Если вы настраиваете интеграцию с PT AF версии 4.2.1 и выше, вам необходимо:

- Добавить в PT Email Security источник с типом **ICAP-сервер**.
- В PT AF добавить ICAP-сервер.
- В шаблоне политики безопасности PT AF настроить правило **Отправлять файлы на ICAP-серверы**.

Если вы настраиваете интеграцию с PT AF версии 3, вам необходимо:

- Добавить в PT Email Security источник с типом **ICAP-сервер**.
- В PT AF настроить работу со сторонними ICAP-службами.

При настройке ICAP-клиента вам необходимо указать ссылку для обращения к ICAP-серверу PT Email Security. Вид ссылки зависит от режима проверки объектов и режима работы ICAP-сервера:

- Ссылки для проверки объектов в блокирующем режиме:
 - REQMOD: `icap://<IP-адрес>:<Порт>/scanrequest?modify=y&block-unwanted=<Блокировать потенциально опасные>&timeout=<Тайм-аут>`
 - RESPMOD: `icap://<IP-адрес>:<Порт>/scanresponse?modify=y&block-unwanted=<Блокировать потенциально опасные>&timeout=<Тайм-аут>`

Примечание. В параметре `block-unwanted` вы можете указать `y`, если необходимо блокировать потенциально опасные файлы, или `n` — если блокировать такие файлы не требуется (по умолчанию потенциально опасные файлы не блокируются). В параметре `timeout` вы можете указать тайм-аут ответа ICAP-сервера в секундах (по умолчанию 30 секунд).
- Ссылки для проверки объектов в режиме ожидания:
 - REQMOD: `icap://<IP-адрес>:<Порт>/scanrequest?modify=no&timeout=<Тайм-аут>`
 - RESPMOD: `icap://<IP-адрес>:<Порт>/scanresponse?modify=no&timeout=<Тайм-аут>`
- Ссылки для проверки объектов в пассивном режиме:
 - REQMOD: `icap://<IP-адрес>:<Порт>/bypass`
 - RESPMOD: `icap://<IP-адрес>:<Порт>/bypass`

Добавление источника в PT Email Security

► Чтобы добавить источник в PT Email Security:

1. В главном меню выберите **Источники**.
2. Нажмите кнопку **Добавить источник**.

3. В поле **Название** введите название источника, которое будет указано в свойствах полученных от него объектов.

Название должно содержать не менее пяти символов и быть уникальным среди названий всех источников. Название может содержать только строчные буквы латинского алфавита, цифры, дефис и при этом начинаться и заканчиваться только буквами.

4. В раскрывающемся списке **Тип** выберите **ICAP-сервер**.
5. Если необходимо, в поле **IP-адреса ICAP-сервера** введите дополнительные адреса.

Примечание. В поле указан IP-адрес ICAP-сервера, создаваемого в PT Email Security. Он понадобится вам при настройке интеграции в PT AF.

6. Если необходимо, измените стандартный порт подключения к ICAP-серверу.

Внимание! Указанный порт не должен использоваться другими источниками для проверки, службами или приложениями ОС.

7. Если необходимо принимать объекты только с определенных адресов, включите фильтрацию входящих подключений и укажите IP-адреса разрешенных узлов или подсетей.
8. Нажмите кнопку **Добавить источник**.

Источник добавлен в PT Email Security.

14.4. PT ISIM 5.2 и выше

При интеграции продуктов PT ISIM отправляет извлеченные из сетевого трафика файлы на проверку в PT Email Security через публичный API. При выявлении опасных или потенциально опасных объектов в PT ISIM регистрируется событие информационной безопасности, которое будет доступно для анализа в цепочках инцидентов.

Внимание! Если в вашей информационной системе используется межсетевой экран или другие средства контроля сетевого трафика, требуется настроить в них правила, разрешающие передачу трафика через порты TCP 80, 443 от узла PT ISIM к основному узлу PT Email Security.

Примечание. Инструкции по настройке PT ISIM приведены [в технической документации продукта](#).

Для настройки интеграции в PT Email Security необходимо:

- Выпустить токен доступа к публичному API с разрешенным действием **Проверка с параметрами источника**.
- Добавить в PT Email Security источник с типом **API с выбранными параметрами проверки**.

Для настройки интеграции в PT ISIM необходимо настроить отправку объектов в PT Email Security.

Добавление источника в PT Email Security

► Чтобы добавить источник в PT Email Security:

1. В главном меню выберите **Источники**.
2. Нажмите кнопку **Добавить источник**.
3. В поле **Название** введите название источника, которое будет указано в свойствах полученных от него объектов.

Название должно содержать не менее пяти символов и быть уникальным среди названий всех источников. Название может содержать только строчные буквы латинского алфавита, цифры, дефис и при этом начинаться и заканчиваться только буквами.
4. В раскрывающемся списке **Тип** выберите **API с выбранными параметрами проверки**.
5. В раскрывающемся списке **Токен доступа** выберите токен доступа к публичному API.
6. Нажмите кнопку **Добавить источник**.

Источник добавлен в PT Email Security.

14.5. PT NAD 7.1 и выше

При интеграции продуктов PT NAD отправляет извлеченные из трафика файлы на проверку в PT Email Security и получает результаты проверки. Информация об обнаруженных угрозах отображается в карточках сессий и атак, а также в таблицах сессий и атак в столбце с метками репутации.

Внимание! Если в вашей информационной системе используется межсетевой экран или другие средства контроля сетевого трафика, требуется настроить в них правила, разрешающие передачу трафика через порт TCP 2344 от узла PT NAD к основному узлу PT Email Security.

Интеграция осуществляется по ICAP. При этом PT Email Security является ICAP-сервером. В качестве ICAP-клиента в PT NAD используется модуль `ptdri-worker@icap`. Он отправляет извлеченные из трафика файлы на проверку и получает результаты проверки. В PT Email Security также отправляется дополнительная информация о файлах, например протокол, по которому перехвачен файл, и IP-адреса узлов, между которыми он передавался.

Примечание. Инструкции по настройке PT NAD приведены [в технической документации продукта](#).

Для настройки интеграции необходимо:

- В PT Email Security добавить источник с типом **PT NAD**.
- В центре управления PT NAD в параметрах интеграции с PT Email Security указать параметры созданного ICAP-сервера.

Добавление источника в PT Email Security

► Чтобы добавить источник в PT Email Security:

1. В главном меню выберите **Источники**.
2. Нажмите кнопку **Добавить источник**.
3. В поле **Название** введите название источника, которое будет указано в свойствах полученных от него объектов.

Название должно содержать не менее пяти символов и быть уникальным среди названий всех источников. Название может содержать только строчные буквы латинского алфавита, цифры, дефис и при этом начинаться и заканчиваться только буквами.

4. В раскрывающемся списке **Тип** выберите **PT NAD**.
5. Если необходимо, в поле **IP-адреса ICAP-сервера** введите дополнительные адреса.

Примечание. В поле указан IP-адрес ICAP-сервера, создаваемого в PT Email Security. Он понадобится вам при настройке интеграции в PT NAD.

6. Если необходимо, измените стандартный порт подключения к ICAP-серверу.

Внимание! Указанный порт не должен использоваться другими источниками для проверки, службами или приложениями ОС.

7. Если необходимо принимать объекты только с определенных адресов, включите фильтрацию входящих подключений и укажите IP-адреса разрешенных узлов или подсетей.
8. Нажмите кнопку **Добавить источник**.

Источник добавлен в PT Email Security.

14.6. PT NGFW 1.8 и выше

При интеграции продуктов PT NGFW отправляет в PT Email Security извлеченные из трафика HTTP-сообщения и файлы для проверки. В случае выявления угрозы PT NGFW блокирует соответствующий трафик.

Внимание! Если в вашей информационной системе используется межсетевой экран или другие средства контроля сетевого трафика, требуется настроить в них правила, разрешающие передачу трафика через порт TCP 1344 от узла PT NGFW к основному узлу PT Email Security.

Интеграция осуществляется по протоколу ICAP. При этом PT Email Security является ICAP-сервером, а PT NGFW — ICAP-клиентом, который отправляет извлеченные из трафика HTTP-сообщения и файлы на проверку и получает результаты проверки.

Для настройки интеграции в PT Email Security необходимо добавить источник с типом **ICAP-сервер**.

Примечание. Инструкции по настройке PT NGFW приведены [в технической документации продукта](#).

Для настройки интеграции в PT NGFW необходимо:

- Добавить ICAP-сервер и указать в его профиле:
 - IP-адрес ICAP-сервера, созданного при добавлении источника в PT Email Security.
 - Ссылки для обращения к ICAP-серверу PT Email Security.
- Создать профиль ICAP и выбрать в нем профиль добавленного ICAP-сервера.
- В правиле безопасности указать созданный профиль ICAP в качестве профиля безопасности. На ICAP-сервер будет отправляться трафик, который соответствует этому правилу безопасности.

Вид ссылки для обращения к ICAP-серверу PT Email Security зависит от режима проверки объектов и режима работы ICAP-сервера:

- Ссылки для проверки объектов в блокирующем режиме:
 - REQMOD: /scanrequest?modify=y&block-unwanted=<Блокировать потенциально опасные>&timeout=<Тайм-аут>
 - RESPMOD: /scanresponse?modify=y&block-unwanted=<Блокировать потенциально опасные>&timeout=<Тайм-аут>

Примечание. В параметре block-unwanted вы можете указать y, если необходимо блокировать потенциально опасные файлы, или n, если блокировать такие файлы не требуется (по умолчанию потенциально опасные файлы не блокируются). В параметре timeout вы можете указать тайм-аут ответа ICAP-сервера в секундах (по умолчанию — 30 секунд).

- Ссылки для проверки объектов в режиме ожидания:
 - REQMOD: /scanrequest?modify=no&timeout=<Тайм-аут>
 - RESPMOD: /scanresponse?modify=no&timeout=<Тайм-аут>
- Ссылки для проверки объектов в пассивном режиме:
 - REQMOD: /bypass
 - RESPMOD: /bypass

Добавление источника в PT Email Security

► Чтобы добавить источник в PT Email Security:

1. В главном меню выберите **Источники**.
2. Нажмите кнопку **Добавить источник**.
3. В поле **Название** введите название источника, которое будет указано в свойствах полученных от него объектов.

Название должно содержать не менее пяти символов и быть уникальным среди названий всех источников. Название может содержать только строчные буквы латинского алфавита, цифры, дефис и при этом начинаться и заканчиваться только буквами.

4. В раскрывающемся списке **Тип** выберите **ICAP-сервер**.
5. Если необходимо, в поле **IP-адреса ICAP-сервера** введите дополнительные адреса.
Примечание. В поле указан IP-адрес ICAP-сервера, создаваемого в PT Email Security. Он понадобится вам при настройке интеграции в PT NGFW.
6. Если необходимо, измените стандартный порт подключения к ICAP-серверу.
Внимание! Указанный порт не должен использоваться другими источниками для проверки, службами или приложениями ОС.
7. Если необходимо принимать объекты только с определенных адресов, включите фильтрацию входящих подключений и укажите IP-адреса разрешенных узлов или подсетей.
8. Нажмите кнопку **Добавить источник**.

Источник добавлен в PT Email Security.

14.7. PT Threat Analyzer 2.10 и выше

При интеграции продуктов PT Email Security отправляет в PT Threat Analyzer результаты заданий, в которых обнаружены опасные или потенциально опасные файлы. Вы также можете настроить отправку найденных в этих заданиях файлов с угрозами. На основе полученных результатов для каждого задания в PT Threat Analyzer формируется отдельный отчет. Интеграция осуществляется через публичный REST API PT Threat Analyzer.

Внимание! Если в вашей информационной системе используется межсетевой экран или другие средства контроля сетевого трафика, требуется настроить в них правила, разрешающие передачу трафика через порты TCP 80, 443 от основного узла PT Email Security к узлу PT Threat Analyzer.

Примечание. Инструкции по настройке PT Threat Analyzer приведены [в технической документации продукта](#).

Для настройки интеграции в PT Threat Analyzer необходимо:

1. Создать учетную запись для PT Email Security.
2. Выпустить ключ API с привилегиями **Загрузка артефактов, Регистрация и изменение отчетов, Регистрация и изменение наблюдений, Просмотр задач обогащения, Создание задач обогащения** для доступа к REST API.
3. Добавить экземпляр источника с типом PT Email Security.
4. Привязать созданный источник к учетной записи PT Email Security.

Для настройки интеграции в PT Email Security необходимо настроить отправку данных для отчетов в PT Threat Analyzer.

Настройка PT Email Security для отправки данных для отчетов

► Чтобы настроить отправку данных для отчетов в PT Threat Analyzer:

1. В главном меню выберите **Система** → **Основные параметры**.
2. В блоке параметров **Отправка данных в PT Threat Analyzer** включите отправку данных.
3. В поле **URL-адрес PT Threat Analyzer** введите адрес REST API PT Threat Analyzer в формате `https://<Доменное имя или IP-адрес>`.
4. В поле **Ключ API** введите ключ для доступа к REST API PT Threat Analyzer.
5. В раскрывающемся списке **Уровень доступа** выберите уровень доступа пользователя в PT Threat Analyzer, который необходим для доступа к отчету.
6. С помощью переключателя **Отправка файлов** настройте отправку файлов:
 - Если отправлять файлы не требуется, выберите **Не отправлять**.
 - Если требуется отправлять только опасные и потенциально опасные файлы, выберите **Только файлы с угрозами**.
 - Если требуется также отправлять файлы, в которых содержатся обнаруженные файлы с угрозами (например, архивы или письма), выберите **Файлы с угрозами и связанные с ними файлы**.
7. Нажмите кнопку **Сохранить**.

Отправка данных для отчетов в PT Threat Analyzer настроена.

15. Настройка обновления PT Email Security

Обновление PT Email Security включено по умолчанию, новые версии устанавливаются автоматически. Вы можете настроить автоматическое обновление или отключить его, чтобы запускать обновление вручную.

Новые версии PT Email Security бывают двух типов: с новыми функциями и с исправлениями. При обновлении до версии с новыми функциями в PT Email Security появляются новые возможности. Обновление до версии с исправлениями происходит в рамках текущей версии и предназначено для устранения ошибок. Вы можете настроить автоматическое обновление для версий обоих типов или автоматическое обновление только для версий с исправлениями.

Управлять обновлением можно на странице **Система** → **Обновления**. На этой странице вы можете просмотреть текущую версию PT Email Security, проверить наличие новых версий, запустить ручное обновление или перейти на страницу настройки автоматического обновления системы.

 Проверить наличие обновлений

Проверено 14 апреля, 13:40

Доступна версия 5.22.0.110634
От 14 апреля
Обновить сейчас Будет установлена автоматически 16 апреля (среда) в 20:33

Доступна версия 5.22.0.110625
От 14 апреля
Обновить сейчас

Текущая версия
5.22.0.110552

☒ **Автоматическое обновление**
[Изменить](#)
Версии с новыми функциями **Включено**
Не устанавливать версии, которым меньше 30 дней
Расписание
Суббота, 04:00
Версии с исправлениями **Включено**
Не устанавливать версии, которым меньше 24 часов
Расписание
Вторник, 04:00
Среда, 04:00
Пятница, 04:00

Рисунок 8. Страница **Обновления**

В рабочей области страницы расположены:

- Кнопка **Проверить наличие обновлений** для проверки доступных для установки версий.
- Блок с версией, которая доступна для установки. При наличии нескольких доступных версий каждая отображается в отдельном блоке. В блоке также отображается кнопка **Обновить сейчас** для установки версии вручную.
- Блок для настройки автоматического обновления. В блоке отображаются ссылка **Изменить**, настроенные параметры обновления и расписание автоматического обновления для версий с новыми функциями и версий с исправлениями.

Настройка автоматического обновления

Вы можете настроить автоматическое обновление для всех новых версий: и для версий с новыми функциями, и для версий с исправлениями.

► Чтобы настроить автоматическое обновление:

1. В главном меню выберите **Система** → **Обновления**.
2. В блоке параметров **Автоматическое обновление** нажмите ссылку **Изменить**.
3. Включите автоматическое обновление в блоке **Версии с новыми функциями**.
4. Если вы хотите настроить минимальный срок, который должен пройти с момента выхода версии с новыми функциями:
 - В блоке **Версии с новыми функциями** установите флажок **Не устанавливать версии, которым меньше <количество> дней**.
 - Укажите количество дней, по истечении которого нужно установить обновление.
5. Если вы хотите настроить расписание обновления для версий с новыми функциями:
 - В блоке **Версии с новыми функциями** нажмите кнопку **Добавить**.
 - Выберите день недели и укажите время, в которые будут устанавливаться обновления.
6. Если вы хотите настроить минимальный срок, который должен пройти с момента выхода новой версии с исправлениями:
 - В блоке **Версии с исправлениями** установите флажок **Не устанавливать версии, которым меньше <количество> часов**.
 - Укажите количество часов, по истечении которого нужно установить обновление.
7. Если вы хотите настроить расписание обновления для версий с исправлениями:
 - В блоке **Версии с исправлениями** нажмите кнопку **Добавить**.
 - Выберите день недели и укажите время, в которые будут устанавливаться обновления.
8. Нажмите кнопку **Сохранить**.

Настройка автоматического обновления только для версий с исправлениями

Вы можете настроить автоматическое обновление только для версий с исправлениями, отключив автоматическое обновление для версий с новыми функциями.

- ▶ Чтобы настроить автоматическое обновление только для версий с исправлениями:
 1. В главном меню выберите **Система** → **Обновления**.
 2. Нажмите ссылку **Изменить** в блоке **Автоматическое обновление**.
 3. Выключите автоматическое обновление в блоке **Версии с новыми функциями**.
 4. Если вы хотите настроить минимальный срок, который должен пройти с момента выхода новой версии с исправлениями:
 - В блоке **Версии с исправлениями** установите флажок **Не устанавливать версии, которым меньше <количество> часов**.
 - Укажите количество часов, по истечении которого нужно установить обновление.
 5. Если вы хотите настроить расписание обновления для версий с исправлениями:
 - В блоке **Версии с исправлениями** нажмите кнопку **Добавить**.
 - Выберите день недели и укажите время, в которые будут устанавливаться обновления.
 6. Нажмите кнопку **Сохранить**.

Отключение автоматического обновления

- ▶ Чтобы отключить автоматическое обновление:
 1. В главном меню выберите **Система** → **Обновления**.
 2. В блоке параметров **Автоматическое обновление** выключите обновление.

Запуск обновления вручную

- ▶ Чтобы запустить обновление вручную:
 1. В главном меню выберите **Система** → **Обновления**.
 2. Нажмите кнопку **Проверить наличие обновлений**.
 3. В оповещении о новой версии нажмите кнопку **Обновить сейчас**.

Во время обновления все функции PT Email Security будут доступны. По окончании обновления в меню информации о продукте отобразится уведомление об успешном обновлении.

16. Просмотр конфигурации PT Email Security

На страницах раздела **Система** → **Конфигурация** вы можете получить общее представление о настроенной конфигурации PT Email Security: об узлах, входящих в конфигурацию, их IP-адресах и ролях, о развернутых на узлах компонентах и подах. Вы также можете оценить работоспособность конфигурации, увидеть, какие из узлов, компонентов или подов не работают или работают частично, и принять решения по улучшению их работоспособности.

Примечание. В PT Email Security используется микросервисная архитектура и контейнеризация приложений на основе технологий containerd и Kubernetes (K8s). Для просмотра докер-контейнеров и докер-образов вы можете использовать утилиты `crictl` и `ctr`. Утилиты доступны на узлах PT Email Security.

В верхней части каждой страницы указаны:

- Статус отказоустойчивого кластера (отображается, если такой кластер настроен).
- Виртуальный IP-адрес отказоустойчивого кластера (отображается, если такой кластер настроен).
- Общее количество узлов для поведенческого анализа файлов и количество доступных узлов (отображается, если часть узлов недоступна).
- Общее количество виртуальных машин, которые можно запустить на всех узлах для поведенческого анализа файлов, и количество доступных для запуска виртуальных машин (отображается, если часть виртуальных машин недоступна).

Содержимое рабочей области зависит от выбранной страницы.

Страница «Компоненты»

Для просмотра информации о компонентах PT Email Security предназначена страница **Система** → **Конфигурация** → **Компоненты**.

Отказоустойчивый кластер

Настроен

Адрес кластера

10.120.10.120

Узлы для поведенческого анализа

1

ВМ для поведенческого анализа

2

Название	↓↑	Тип	↓↑	Узел	↓↑	Пространство имен	↓↑	Работающих подов	↓↑	Статус	↑
vmagent		Служба мониторинга		ptms-astra-all-qa4		monitoring		0 из 1		Не работает	
prometheus-adapter		Служба мониторинга		ptms-astra-all-qa4		monitoring		11 из 12		Работает частично	
telemetry		Служба интеграции		ptms-astra-all-qa4		ptms		2		Работает	
ptioc		Средство проверки		ptms-astra-node3-q...		ptms		2		Работает	
ptcategorizer		Средство проверки		ptms-astra-node3-q...		ptms		2		Работает	
cluster-babysitter		Служба обновления		ptms-astra-all-qa4		ptms		1		Работает	
av-nano		Средство проверки		ptms-astra-node3-q...		ptms		4		Работает	
mc-licensing		Служба		ptms-astra-node3-q...		ptmc		1		Работает	
kube-state-metrics		Служба мониторинга		ptms-astra-all-qa4		monitoring		1		Работает	

Рисунок 9. Страница **Компоненты**

В рабочей области страницы расположена таблица с информацией о компонентах PT Email Security. По кнопке **↓↑** в заголовке любого столбца таблицы вы можете отсортировать компоненты по значениям в этом столбце. Нажимая на заголовок столбца, вы можете отфильтровать содержимое таблицы по значениям в столбце. Для каждого компонента в таблице указаны:

- **Название.**
- **Тип** — назначение компонента.
- **Узел** — название узла, на котором развернут компонент.
- **Пространство имен:**
 - **ptms** — PT Email Security.
 - **ptmc** — PT MC.
 - **monitoring** — подсистема мониторинга работы PT Email Security.
- **Работающих подов** — количество работающих подов и общее количество подов, используемых компонентом.
- **Статус** — один из статусов пода: **Работает**, **Работает частично** или **Не работает**.

Страница «Узлы»

Для просмотра информации о входящих в конфигурацию PT Email Security узлах и ролях этих узлов предназначена страница **Система** → **Конфигурация** → **Узлы**.

Отказоустойчивый кластер

Настроен

Адрес кластера

10.120.10.120

Узлы для поведенческого анализа

1

ВМ для поведенческого анализа

2

ptms-astra-node3

Работает

scan-core

backend

persistent-data

control-plane

IP-адрес

ЦП

ОЗУ

ОС

containerd

Kubernetes

Поды

10.120.4.143

6 ядер

15,62 ГБ

Astra Linux

1.6.20

v1.26.4

30

ptms-astra-node2

Работает

scan-core

backend

persistent-data

control-plane

IP-адрес

ЦП

ОЗУ

ОС

containerd

Kubernetes

Поды

10.120.4.142

6 ядер

15,62 ГБ

Astra Linux

1.6.20

v1.26.4

22

ptms-astra-sandbox

Работает

sandbox

IP-адрес

ЦП

ОЗУ

ОС

containerd

Kubernetes

Xen

Поды

ВМ

10.120.4.149

16 ядер

26,47 ГБ

Astra Linux

1.6.20

v1.26.4

4.16.5

15

2

Рисунок 10. Страница **Узлы**

В рабочей области страницы расположены панели с информацией об узлах, входящих в конфигурацию PT Email Security. Для каждого узла указаны:

- Имя ноды Kubernetes и имя узла (если оно отличается от имени ноды).
- Роли узла. Могут быть настроены следующие роли:
 - **backend** — сервер приложений. На таком сервере могут быть установлены: встроенный PT MC, служба обновлений, служба публичного API и другие компоненты PT Email Security.
 - **control-plane** — основной или резервный узел с управляющей нодой Kubernetes.
 - **persistent-data** — хранилище файлов.
 - **sandbox** — узел для поведенческого анализа.
 - **scan-core** — ядро проверки PT Email Security.
- **IP-адрес** — IP-адрес узла.
- **ЦП** — количество ядер центрального процессора.
- **ОЗУ** — объем памяти.
- **ОС** — версия операционной системы.
- **containerd** — версия среды containerd.
- **Kubernetes** — версия Kubernetes.
- **Xen** — версия гипервизора Xen.

- **Поды** — количество подов, развернутых на узле.
- **ВМ** — количество виртуальных машин, которые можно запустить на узле для поведенческого анализа файлов.
- Статус узла: **Работает**, **Есть ошибки** или **Недоступен**.

Страница «Поды»

Для просмотра информации о подах Kubernetes предназначена страница **Система** → **Конфигурация** → **Поды**.

Отказоустойчивый кластер Настроен		Адрес кластера 10.120.10.120		Узлы для поведенческого анализа 1		ВМ для поведенческого анализа 2	
Имя пода	Компонент	Узел	Перезапусков	Время работы	Работающих контейн...	Статус	
os-installer-xffsn	os-installer	ptms-astra-node3	2	2 д 4 ч	0	Не работает	
prometheus-adapt...	prometheus-adapter	ptms-astra-node3	2	3 нед 5 д	1	Работает	
trace2ml-6746f74c...	trace2ml	ptms-astra-node4	0	3 ч 1 мин	1	Работает	
trace2ml-6746f74c...	trace2ml	ptms-astra-node3	0	3 ч 1 мин	1	Работает	
ptioc-7cc7bb44bc-...	ptioc	ptms-astra-node3	0	3 ч 22 мин	1	Работает	
ptioc-7cc7bb44bc-...	ptioc	ptms-astra-node3	0	3 ч 21 мин	1	Работает	
ptcategorizer-c6d4...	ptcategorizer	ptms-astra-node4	0	3 ч 24 мин	1	Работает	
ptcategorizer-c6d4...	ptcategorizer	ptms-astra-node3	0	3 ч 23 мин	1	Работает	
cluster-babysitter-...	cluster-babysitter	ptms-astra-node4	0	3 ч 26 мин	2	Работает	

Рисунок 11. Страница **Поды**

В рабочей области страницы расположена таблица с информацией о подах Kubernetes. По кнопке  в заголовке любого столбца таблицы вы можете отсортировать поды по значениям в этом столбце. Нажимая на заголовок столбца, вы можете отфильтровать содержимое таблицы по значениям в столбце. Для каждого пода в таблице указаны:

- **Имя**.
- **Компонент** — название компонента, использующего под.
- **Узел** — название узла, на котором развернут под.
- **Перезапусков** — количество перезапусков пода.
- **Время работы** — общее время работы пода.
- **Работающих контейнеров** — количество контейнеров, работающих внутри пода.
- **Статус** — один из статусов пода: **Работает**, **Не работает**.

17. Мониторинг системных ресурсов в Grafana

Для визуализации данных об использовании системных ресурсов на узлах PT Email Security используется средство визуализации и мониторинга данных Grafana с набором стандартных дашбордов. Для работы с Grafana в главном меню вам необходимо выбрать раздел **Система** → **Конфигурация** → **Мониторинг**. Страница Grafana открывается в отдельной вкладке браузера. На странице отображается дашборд, выбранный основным. Работа Grafana одновременно на нескольких вкладках не поддерживается.

Примечание. По умолчанию установлена темная тема оформления интерфейса. Вы можете сменить тему оформления на светлую в параметрах профиля пользователя.

При работе с Grafana вы можете:

- Просматривать информацию на основном дашборде.
- Выбирать для просмотра другие стандартные дашборды.
- Копировать стандартные дашборды и при необходимости изменять их.
- Создавать и импортировать новые дашборды.
- Настраивать почтовые уведомления по событиям для любого дашборда.

Внимание! Для получения уведомлений от Grafana по электронной почте вам необходимо на основном узле PT Email Security настроить подключение к SMTP-серверу.

Инструкции по работе с Grafana вы можете найти в технической документации Grafana.

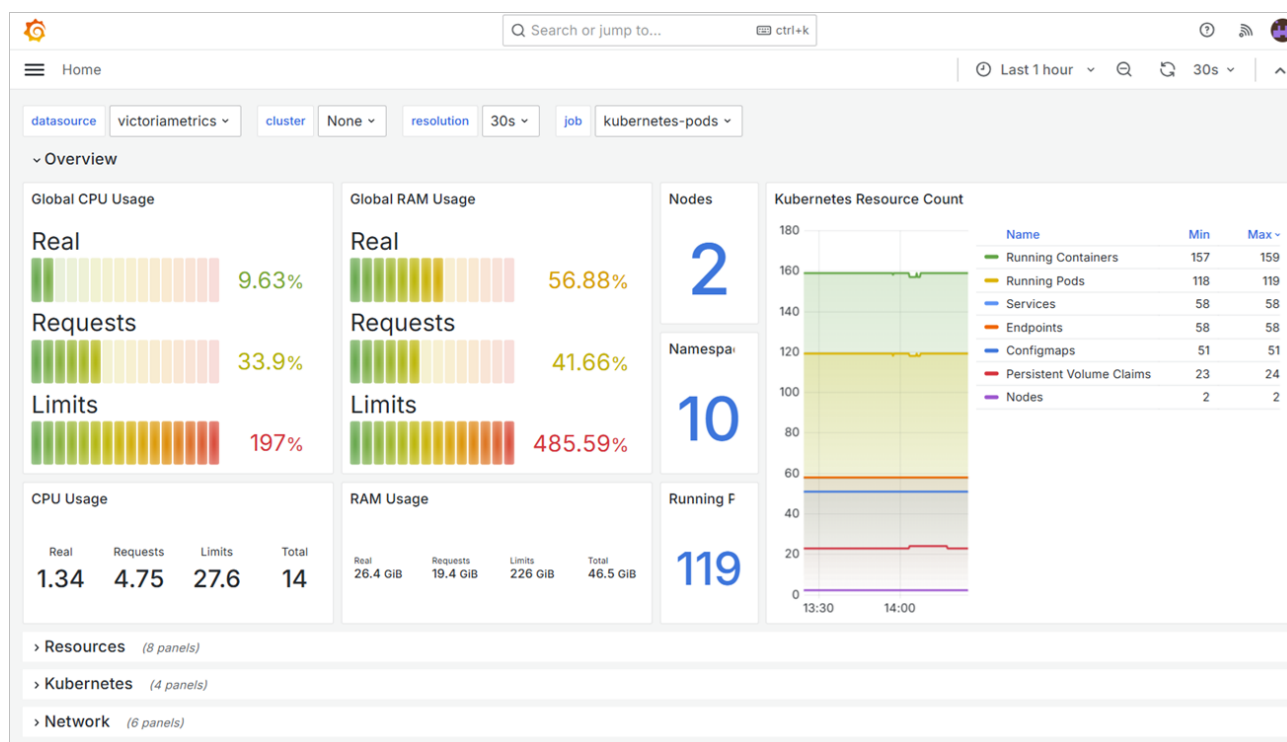


Рисунок 12. Мониторинг системных ресурсов в Grafana

В верхней части страницы расположена панель инструментов с кнопками:

☰ — для открытия боковой панели с главным меню. Используя разделы главного меню, вы можете переходить на страницы Grafana:

- **Home** — для просмотра домашней страницы с основным дашбордом.
- **Starred** — для выбора избранных дашбордов.
- **Dashboards** — для работы с дашбордами.
- **Explore** — для создания запросов к источникам данных.
- **Alerting** — для работы с уведомлениями.

🕒 — для выбора периода времени, за который отображаются данные на виджетах.

↻ — для обновления данных на виджетах.

⌵ — для настройки автоматического обновления данных на виджетах.

В рабочей области страницы отображаются виджеты выбранного вами дашборда. Виджеты сгруппированы в раскрывающиеся блоки.

Назначение стандартных дашбордов

Для мониторинга обработки объектов в PT Email Security предназначены дашборды:

- **Product / Rabbitmq / Queues** — предоставляет детализированные данные об очередях сообщений компонента RabbitMQ, включая общее количество очередей, динамику изменения количества сообщений в очередях, а также скорость поступления, доставки и подтверждения сообщений.
- **Product / Gateway / BCC** — предназначен для мониторинга обработки писем от источников типа «Почтовый сервер в режиме фильтрации» и «Почтовый сервер в режиме зеркалирования».

В блоке **Current rates** отображаются график изменения режимов работы источников во времени. Для каждого источника фиксируются переходы между блокирующим и пассивным режимами, что позволяет отследить стабильность их работы.

В блоке **Incoming Emails Stats** отображается статистика приема писем. Представлен график по времени, отражающий динамику изменения количества писем, полученных от каждого источника. Также представлены диаграммы, показывающие распределение общего количества писем по источникам и их типам.

В блоке **Processed Emails Stats** отображается статистика обработки писем.

Представлена гистограмма, показывающая распределение количества писем по времени их обработки, что позволяет оценить общую нагрузку и типичную продолжительность обработки письма.

Также представлены графики, отражающие динамику изменения во времени следующих показателей: количества писем, для которых выполнено определенное действие (пропущено, заблокировано), и количества писем, обработанных без таких действий; количества писем с определенными статусом, вердиктом и причиной вердикта (отдельные графики для пропущенных и заблокированных писем и для писем, обработанных без таких действий); количества обработанных писем от каждого источника.

Примечание. Письмо считается заблокированным, если оно заблокировано хотя бы для одного получателя. На графиках и диаграммах для писем, обработанных без выполнения каких-либо действий, учитываются письма только от источников типа «Почтовый сервер в режиме зеркалирования».

Кроме того, представлены диаграммы, показывающие распределение общего числа обработанных писем: по именам источников (отдельные диаграммы для пропущенных и заблокированных писем и для писем, обработанных без таких действий); по действиям (пропущено, заблокировано или обработано без таких действий); по статусам обработки (успешно или с ошибкой); отдельно для писем без задания на проверку — по действиям (пропущено или заблокировано).

В блоке **Errors Stats** отображается статистика ошибок при обработке писем.

Представлены графики, отражающие динамику изменения во времени количества ошибок с определенными типами и кодами. Также приведены диаграммы, показывающие распределение общего количества ошибок по типам и кодам. Даны отдельные графики и диаграммы для ошибок, возникших при попытке отправить письмо на внешний почтовый сервер, и ошибок, возвращенных удаленным сервером в ответ на отправку.

Для фильтрации данных в панели инструментов дашборда можно выбрать тип и название источника.

- **Product / BA Queue** — дашборд предназначен для мониторинга состояния и производительности модуля поведенческого анализа.

В блоке **Current queue size** отображаются текущее количество файлов в очереди на поведенческий анализ (добавленных и проверяемых), продолжительность анализа, количество запущенных для анализа ВМ, история изменения длины очереди и распределение накладных расходов по временным диапазонам.

Блок **Total stats** содержит статистику запусков поведенческого анализа за выбранный период: распределение по источникам, типам файлов и образам ВМ, количество ошибок и показатели эффективности кэширования.

В блоке **Rates in time** представлены графики по времени, отражающие динамику ошибок, накладных расходов, использования ВМ, запусков поведенческого анализа по источникам, типам файлов и образам ВМ, а также показатели активности кэша и количества успешно завершенных запусков.

Для фильтрации данных в панели инструментов дашборда можно выбрать источники, образы ВМ и типы файлов.

Для мониторинга узлов PT Email Security предназначен дашборд:

- **Node Exporter Full** — предоставляет детализированные данные о состоянии узлов PT Email Security, включая загрузку центрального процессора, использование памяти ОЗУ, состояние файловых систем и сетевой трафик.

Для мониторинга компонентов PT Email Security предназначены дашборды:

- **RabbitMQ-Overview** — дашборд предоставляет сводную информацию о работе компонента RabbitMQ, включая количество очередей, сообщений, соединений, каналов и узлов, а также скорость поступления, доставки, подтверждения и повторной отправки сообщений. Кроме того, дашборд предоставляет данные об использовании компонентом системных ресурсов, включая память ОЗУ, дисковое пространство, файловые дескрипторы и сокеты.
- **VictoriaMetrics — cluster** — предоставляет информацию о загрузке центрального процессора, использовании памяти ОЗУ и дискового пространства в кластере системы VictoriaMetrics.
- **VictoriaMetrics — vmagent** — отображает информацию о работе агента сбора данных vmagent системы VictoriaMetrics, включая объем передаваемых данных и задержки их обработки.

В PT Email Security используется микросервисная архитектура и контейнеризация приложений на основе технологий containerd и Kubernetes. Для мониторинга работы кластера Kubernetes предназначены дашборды:

- **kube-state-metrics-v2** — отображает состояние объектов Kubernetes, включая узлы, поды, развертывания (Deployments), наборы подов с состоянием (Statefulset), контейнеры, автоскейлеры, задания и постоянные хранилища.
- **Kubernetes / System / API Server** — предназначен для мониторинга производительности API-сервера Kubernetes, включая нагрузку на обработку запросов и задержки операций.
- **Kubernetes / Views / Global** — предоставляет сводную информацию о загрузке ресурсов и состоянии всех компонентов кластера Kubernetes (основной дашборд по умолчанию).
- **Kubernetes / Views / Namespaces** — показывает использование ресурсов и количество активных подов в разрезе пространств имен.
- **Kubernetes / Views / Nodes** — отображает данные о производительности и загрузке узлов Kubernetes, включая центральный процессор, память ОЗУ и сетевые ресурсы.
- **Kubernetes / Views / Pods** — предоставляет информацию о статусе подов, использовании ими ресурсов и возможных причинах перезапусков.
- **Kubernetes Cluster Monitoring** — отображает данные о состоянии кластера Kubernetes, включая работу сервисов и использование вычислительных ресурсов.
- **Kubernetes Metrics — Deployments vs StatefulSets vs DaemonSets** — предназначен для просмотра информации об использовании ресурсов различных типов развертываний в Kubernetes, включая загрузку центрального процессора, использование памяти ОЗУ, дискового пространства, сетевого ввода-вывода и количество недоступных реплик.

Настройка почтовых уведомлений

В Grafana предусмотрена отправка уведомлений по электронной почте для следующих стандартных событий:

- **sb_component_offline** — компонент PT Email Security не работает.
- **sb_component_partially_unavailable** — компонент PT Email Security работает частично.
- **system_update_finished** — завершено обновление компонентов PT Email Security.

Для настройки отправки почтовых уведомлений от Grafana вам необходимо:

- На странице **Alerting** → **Contact points** добавить электронные адреса получателей уведомлений.
- На основном узле PT Email Security настроить подключение к SMTP-серверу.

Уведомления будут отправляться для всех событий на все добавленные адреса. При необходимости вы можете отключить отставку уведомлений для событий на странице **Alerting** → **Silences**.

- Чтобы настроить подключение к SMTP-серверу на основном узле PT Email Security,

выполните команду:

```
sudo ptmsctl system components set -c grafana -p grf-smtp-host=<Доменное имя или IP-адрес SMTP-сервера>:<Порт> -p grf-smtp-user=<Логин> -p grf-smtp-pass=<Пароль> -p grf-smtp-from-address=<Почтовый адрес отправителя>
```

Например:

```
sudo ptmsctl system components set -c grafana -p grf-smtp-host=hostname:587 -p grf-smtp-user=emailsecurity -p grf-smtp-pass=P@ssw0rd -p grf-smtp-from-address=emailsecurity@hostname.ru
```

Таблица 5. Параметры подключения к SMTP-серверу

Параметр	Тип данных	Описание
grf-smtp-from-address	String	Электронный адрес, который будет указан в уведомлении в качестве отправителя
grf-smtp-host	String	IP-адрес или доменное имя SMTP-сервера в формате <Адрес> : <Порт>
grf-smtp-pass	String	Пароль для аутентификации на SMTP-сервере
grf-smtp-skip-tls	Boolean	Требуется ли проверять SSL/TLS-сертификат SMTP-сервера (по умолчанию — false)
grf-smtp-user	String	Логин для аутентификации на SMTP-сервере

18. Смена IP-адреса узла PT Email Security

Смена IP-адресов узлов не поддерживается в конфигурации PT Email Security с отказоустойчивым кластером.

Для смены IP-адреса основного узла в базовой конфигурации PT Email Security вам необходимо:

1. Изменить IP-адрес в ОС на основном узле.

Внимание! Сразу после смены IP-адреса в ОС необходимо на основном узле изменить IP-адрес в параметрах PT Email Security.

2. На основном узле изменить IP-адрес в параметрах PT Email Security.

Для смены IP-адреса основного узла в высоконагруженной конфигурации PT Email Security вам необходимо:

1. Изменить IP-адрес в ОС на основном узле.

Внимание! Сразу после смены IP-адреса в ОС необходимо на основном узле изменить IP-адрес в параметрах PT Email Security.

2. На основном узле изменить IP-адрес в параметрах PT Email Security.
3. На основном узле исключить каждый дополнительный узел из конфигурации PT Email Security.
4. Установить компоненты PT Email Security на каждый дополнительный узел.

Примечание. Если на дополнительном узле уже установлены компоненты PT Email Security, в процессе установки эти компоненты будут проверены и узел будет добавлен в конфигурацию PT Email Security.

Для смены IP-адреса дополнительного узла в высоконагруженной конфигурации PT Email Security вам необходимо:

1. Удалить компоненты PT Email Security с дополнительного узла (с сохранением гипервизора Xen и конфигурационных файлов PT Email Security).
2. Изменить IP-адрес в ОС на дополнительном узле.
3. Повторно установить компоненты PT Email Security на дополнительный узел.

Изменение IP-адреса узла в ОС

► Чтобы изменить IP-адрес узла в ОС:

1. Откройте файл `/etc/hosts`.
2. Укажите в файле новый IP-адрес и сохраните изменения.
3. Откройте файл `/etc/network/interfaces`.

4. Укажите в файле новый IP-адрес и сохраните изменения.

5. Перезапустите службу `networking`:

```
sudo systemctl restart networking
```

Примечание. После перезапуска службы SSH-соединение с узлом будет разорвано. Для продолжения настройки подключитесь к узлу, используя новый IP-адрес.

Изменение IP-адреса основного узла в параметрах PT Email Security

Инструкцию необходимо выполнять на основном узле PT Email Security. Перед сменой IP-адреса основного узла в параметрах PT Email Security необходимо изменить IP-адрес узла в ОС.

► Чтобы изменить IP-адрес основного узла в параметрах PT Email Security:

1. Перейдите в каталог со скриптами установщика PT Email Security:

```
cd /home/user/ptsb-installer
```

2. Запустите скрипт `change-master-node-ip.sh`:

```
sudo ./change-master-node-ip.sh
```

3. По завершении работы скрипта нажмите клавишу Enter.

Узел будет перезагружен.

Исключение дополнительного узла из конфигурации PT Email Security

Инструкцию необходимо выполнять на основном узле PT Email Security.

► Чтобы исключить дополнительный узел из конфигурации PT Email Security:

1. Получите список узлов PT Email Security:

```
sudo kubectl --kubeconfig /etc/kubernetes/admin.conf get node
```

2. Если дополнительный узел указан в списке, исключите его из конфигурации:

```
sudo kubectl --kubeconfig /etc/kubernetes/admin.conf delete node <Имя дополнительного узла>
```

Появится сообщение об удалении дополнительного узла.

Удаление компонентов PT Email Security с дополнительного узла

► Чтобы удалить компоненты PT Email Security с дополнительного узла:

1. Перейдите в каталог со скриптами установщика PT Email Security:

```
cd /home/user/ptsb-installer
```

2. Запустите скрипт `reset-kubernetes.sh`:

```
sudo ./reset-kubernetes.sh
```

Примечание. При таком удалении на узле сохраняются гипервизор Xen и конфигурационные файлы компонентов PT Email Security.

3. По завершении работы скрипта нажмите клавишу Enter.

Узел будет перезагружен.

19. Смена DNS-сервера

В случае изменения адреса DNS-сервера, например при смене подсети, вам необходимо:

- На всех узлах PT Email Security изменить адрес DNS-сервера средствами ОС.
- На основном узле PT Email Security перезапустить службу CoreDNS.

В зависимости от используемых на узле служб управления сетевыми параметрами для смены адреса DNS-сервера в ОС могут использоваться различные файлы, например файлы `/etc/network/interfaces` (параметр `dns-nameservers`) и `/etc/resolv.conf`. Для настройки адреса DNS-сервера в ОС следуйте документации используемых служб.

Внимание! Если файл `/etc/resolv.conf` используется службами ОС, содержимое файла обновляется автоматически. В этом случае все изменения, внесенные вами в этот файл вручную, будут потеряны, что может привести к неработоспособности PT Email Security.

- Чтобы перезапустить службу CoreDNS,

выполните команду:

```
sudo kubectl --kubeconfig /etc/kubernetes/admin.conf -n kube-system rollout restart  
deploy/coredns
```

Появится сообщение:

```
deployment.apps/coredns restarted
```

Служба CoreDNS перезапущена.

20. Резервное копирование и восстановление параметров PT Email Security

Резервная копия параметров PT Email Security создается автоматически при каждом запуске скрипта `install.sh`, файлы резервной копии сохраняются в каталоге `/opt/ptms/var/configuration-backups`. Дополнительно вы можете вручную запустить создание резервной копии параметров. Рекомендуется создавать резервную копию параметров после каждого обновления версии PT Email Security.

При создании резервной копии параметров PT Email Security сохраняются:

- Основные параметры.
- Параметры, заданные с помощью команды `ptmsctl`.
- Параметры антивирусов и средств проверки Positive Technologies.
- Параметры источников и параметры проверки источников, кроме источников с типом «API с выбранными параметрами проверки».

При создании резервной копии не сохраняется лицензия. Если PT Email Security установлен в виртуальной среде, не сохраняются параметры виртуальной машины.

Создание резервной копии параметров PT Email Security

Если вы планируете разворачивать PT Email Security на новом узле или удалять данные с жесткого диска, кроме создания резервной копии параметров вам необходимо:

- Через веб-интерфейс сохранить пользовательские YARA-правила и пользовательские образы ВМ (в случае удаления каталога `/opt/ptms/var/minio`).
- Сохранить данные из каталога `/opt/ptms/var/stolon/postgres`. В нем содержатся, например, данные черного и белого списков, информация о созданных токенах доступа, параметры источников с типом «API с выбранными параметрами проверки».

Примечание. При запуске скриптов для удаления PT Email Security данные из этих каталогов не удаляются.

После обновления версии PT Email Security рекомендуется использовать скрипт для создания резервной копии параметров новой версии. Для получения актуального скрипта вы можете обратиться в техническую поддержку Positive Technologies. Инструкцию необходимо выполнить на основном узле PT Email Security.

► Чтобы создать резервную копию параметров PT Email Security:

1. Перейдите в каталог со скриптами установщика PT Email Security:
`cd /home/user/ptsb-installer`
2. Запустите скрипт `backup-config.sh`, указав полный путь к файлу для сохранения резервной копии параметров:
`sudo ./backup-config.sh --backup-file <Путь к файлу резервной копии>`

Например:

```
sudo ./backup-config.sh --backup-file /opt/ptms/configuration/backup_11-12-2025.yaml
```

Восстановление параметров PT Email Security из резервной копии

Резервную копию параметров можно использовать при переустановке или развертывании PT Email Security на новом узле.

Внимание! Для восстановления параметров из резервной копии имена узлов, версия и конфигурация PT Email Security должны совпадать с теми, для которых была создана резервная копия.

Инструкцию необходимо выполнить на основном узле после завершения развертывания PT Email Security. Для конфигурации с отказоустойчивым кластером должны быть развернуты все три узла кластера.

► Чтобы восстановить параметры PT Email Security из резервной копии:

1. Перейдите в каталог со скриптами установщика PT Email Security:

```
cd /home/user/ptsb-installer
```

2. Запустите скрипт `install.sh`, указав полный путь к файлу резервной копии параметров и серийный номер лицензии PT Email Security:

```
sudo ./install.sh --serial-number '<Серийный номер лицензии>' --backup-file <Путь к файлу резервной копии>
```

Например:

```
sudo ./install.sh --serial-number 'xxxxxx-xxxxxx-xxxxxx-xxxxxx-xxxxxx-xxxxxx-xxxxxx-xxxxxx-xxxxxx-xxxxxx' --backup-file /opt/ptms/var/configuration-backups/backup_11-12-2025.yaml
```

21. Обновление гипервизора Xen

Для обновления гипервизора Xen вам понадобится архив с установщиком PT Email Security.

Примечание. Для получения архива с установщиком актуальной версии PT Email Security вы можете обратиться в техническую поддержку Positive Technologies.

Для обновления гипервизора Xen необходимо:

1. Определить параметры установленного на узле гипервизора Xen.
2. Распаковать на узле архив с установщиком PT Email Security.
3. Если на узле установлен Xen версии 5.21 и ниже или в результате предыдущей попытки обновления произошла ошибка, удалить Xen.
4. Установить на узле новую версию гипервизора Xen.

Определение параметров установленного гипервизора Xen

Перед обновлением вам необходимо определить параметры установленного гипервизора Xen: какое максимальное количество VM запускается на узлах с функцией поведенческого анализа и какой объема памяти выделяется гостевой операционной системе каждой виртуальной машины.

Инструкцию необходимо выполнять на основном узле PT Email Security.

► Чтобы определить параметры установленного гипервизора Xen:

1. Определите максимальное количество VM, запускаемых на узлах с функцией поведенческого анализа:

```
sudo ptmsctl sandbox status
```

Появится таблица со списком узлов и максимальным для них количеством VM.

2. Определите объема памяти, выделяемый гостевой операционной системе каждой виртуальной машины:

```
sudo ptmsctl system components show -c sandbox-creator -p vm_memory_max_mb
```

В столбце `value` появившейся таблицы будет указан объем выделяемой памяти в мегабайтах.

Распаковка архива с установщиком

► Чтобы распаковать архив с установщиком:

1. Скопируйте архив с установщиком в любой каталог на узле.
2. Перейдите в каталог с архивом, например:
`cd /home/user/ptsb-installer`
3. Распакуйте архив, например:
`tar pxf ptsb.installer.debian-12-amd64.5.30.0.177.tar.gz`

Удаление гипервизора Xen

► Чтобы удалить с узла гипервизор Xen:

1. Перейдите в каталог с установщиком PT Email Security, например:
`cd /home/user/ptsb-installer`
2. Запустите скрипт удаления гипервизора Xen:
`sudo ./xen/purge.sh`
3. По завершении работы скрипта нажмите клавишу Enter.
Узел будет перезагружен.
4. Если требуется, введите логин и пароль загрузчика.

Установка гипервизора Xen

Внимание! При установке гипервизора Xen необходимо указать тот же объем оперативной памяти, выделяемый гостевой операционной системе каждой виртуальной машины, что и для установленного ранее гипервизора. При необходимости вы сможете изменить это значение после завершения обновления.

► Чтобы установить гипервизор Xen на узле:

1. Перейдите в каталог с установщиком PT Email Security, например:
`cd /home/user/ptsb-installer`
2. Запустите скрипт установки гипервизора Xen:
 - Если вы устанавливаете гипервизор на основном узле:
`sudo xen/install.sh --vm-count <Количество ВМ> --memory-per-vm <Объем памяти ОС в ГБ>`
 - Если вы устанавливаете гипервизор на дополнительном узле:
`sudo xen/install.sh --slave --vm-count <Количество ВМ> --memory-per-vm <Объем памяти ОС в ГБ>`

Например:

```
sudo xen/install.sh --slave --vm-count 15 --memory-per-vm 2
```
3. По завершении работы скрипта нажмите клавишу Enter.

Узел будет перезагружен.

4. Если требуется, введите логин и пароль загрузчика.

22. Удаление PT Email Security

Вы можете удалить продукт полностью со всех узлов кластера, удалить продукт на определенном узле или функцию поведенческого анализа на определенном узле. Удаление производится с помощью скриптов, которые входят в комплект поставки системы.

► Чтобы удалить PT Email Security:

1. Перейдите в каталог с установщиком:

Например:

```
cd /home/user/ptsb-installer
```

2. Выполните подходящую команду:

- Если требуется удалить продукт вместе с узлами кластера, выполните на каждом узле команду:

```
sudo ./purge-all.sh
```

Примечание. При выполнении команды `sudo ./purge-all.sh` не удаляются данные из БД. Для удаления данных из БД обратитесь в техническую поддержку Positive Technologies.

- Если требуется удалить только продукт без удаления узлов, перейдите на любой основной узел и выполните команду:

```
sudo ./purge-product.sh
```

- Если требуется удалить продукт на определенном узле кластера, перейдите на этот узел и выполните команду:

```
sudo ./purge-kubernetes.sh
```

Внимание! После выполнения команды `sudo ./purge-kubernetes.sh` в односерверной конфигурации потребуется переустановка продукта, так как он перестанет работать.

- Если требуется удалить функцию поведенческого анализа, перейдите на узел, на котором установлена эта функция, и выполните команду:

```
sudo ./xen/purge.sh
```

Примечание. Если функция поведенческого анализа установлена на нескольких узлах, то после выполнения команды она удалится только на том узле, на котором была выполнена команда. Вы также можете отключить функцию поведенческого анализа.

3. Подтвердите удаление.

PT Email Security или функция поведенческого анализа удалены.

23. Диагностика и устранение неисправностей

В этом разделе описываются возможные проблемы в работе PT Email Security и варианты их решения.

Проблемы с действующей лицензией

На странице **Лицензия** отображается сообщение о проблемах с лицензией. Объекты проверяются, но базы средств проверки не обновляются.

Внимание! Вам нужно решить проблему в течение двух недель с момента ее появления. В противном случае проверка объектов прекратится.

Проблема может возникать в следующих случаях:

- С основного узла PT Email Security нет доступа по HTTPS к серверам обслуживания Positive Technologies.
- Служба лицензирования PT Email Security работает некорректно или была остановлена (например, кто-то вручную принудительно завершил ее процесс через консоль ОС).
- Был удален или поврежден файл с информацией о лицензии.
- Изменилась конфигурация узла сервера PT Email Security (например, изменились комплектующие сервера).

Для решения проблемы:

- Проверьте доступ к серверам обслуживания Positive Technologies.
- Обновите информацию о параметрах лицензии на странице **Лицензия**.

Если вам не удалось решить проблему, скачайте файлы журналов PT Email Security и отправьте их в техническую поддержку Positive Technologies.

Не удается заменить лицензию

После замены лицензии, информация о ней не отображается на странице **Лицензия**.

Проблема может возникать в следующих случаях:

- С основного узла PT Email Security нет доступа по HTTPS к серверам обслуживания Positive Technologies.
- Неверно сконфигурирована лицензия.

Для решения проблемы:

- Проверьте доступ к серверам обслуживания Positive Technologies.
- Повторите замену лицензии.

Если вам не удалось решить проблему, скачайте файлы журналов PT Email Security и отправьте их в техническую поддержку Positive Technologies.

После замены лицензии недоступен образ VM

После замены лицензии в параметрах проверки источника стал недоступен образ VM.

Проблема может возникать в случае удаления образа VM из лицензии.

Для решения проблемы в параметрах проверки источника выберите другой образ.

Если вы считаете, что образ VM был удален по ошибке или вам нужно вернуть его в лицензию, обратитесь в техническую поддержку Positive Technologies.

Домен не зарегистрирован

При попытке входа по IP-адресу интерфейс PT Email Security недоступен, отображается сообщение «Домен не зарегистрирован».

Проблема может возникать в следующих случаях:

- Было подключено доменное имя.
- Была настроена трансляция сетевых адресов (NAT).

Для решения проблемы:

- Просмотрите подключенное доменное имя и повторите попытку входа, но уже не по IP-адресу, а по доменному имени.
- Отключите доменное имя и повторите попытку входа по IP-адресу.

Если вам не удалось решить проблему, обратитесь в техническую поддержку Positive Technologies.

Не удастся запустить поведенческий анализ в интерактивном режиме

При попытке запустить поведенческий анализ в интерактивном режиме появляется сообщение о разрыве соединения.

Проблема может возникать, если доступ к интерфейсу PT Email Security выполняется через обратный прокси-сервер (reverse proxy), и на сервере отключено проксирование WebSocket-соединений.

Для решения проблемы настройте на обратном прокси-сервере вашей организации проксирование WebSocket-соединений. Ниже приведен пример настройки для прокси-сервера nginx.

► Чтобы настроить проксирование WebSocket-соединений для обратного прокси-сервера nginx:

1. Откройте конфигурационный файл `/etc/nginx/nginx.conf`.
2. В секцию `location` добавьте строки:
`proxy_http_version 1.1;`

```
proxy_set_header Upgrade $http_upgrade;
proxy_set_header Connection "upgrade";
```

3. Сохраните изменения и закройте файл.
4. Проверьте конфигурацию и примените изменения:


```
sudo nginx -t
sudo systemctl reload nginx
```

Скачивание файлов журналов PT Email Security

Скачать файлы журналов можно через интерфейс PT Email Security. При скачивании файлы журналов добавляются в ZIP-архив с названием `ptms-logs-<Дата и время скачивания>-<Период>.zip`.

- ▶ Чтобы скачать файлы журналов через интерфейс,

в главном меню выберите  → **Скачать файлы журналов** → **<Период>**.

Файлы журналов собраны, добавлены в архив и скачаны на ваш компьютер.

С помощью скрипта из комплекта поставки вы можете собрать файлы журналов и сохранить их локально. Инструкцию необходимо выполнять на основном узле.

- ▶ Чтобы собрать файлы журналов с помощью скрипта:

1. Перейдите в каталог со скриптами установщика PT Email Security:


```
cd /home/user/ptsb-installer
```
2. Запустите скрипт `collect-logs.sh`:


```
sudo ./collect-logs.sh
```

Файлы журналов собраны, добавлены в ZIP-архив и скачаны на ваш компьютер.

Скачивание файлов журналов источника

Вы можете скачать файлы журналов отдельного источника через интерфейс PT Email Security. При скачивании файлы журналов добавляются в ZIP-архив с названием `ptms-logs-<Дата и время скачивания>-<Период>.zip`.

- ▶ Чтобы скачать файлы журналов источника:

1. В главном меню выберите **Источники**.
2. Нажмите на панель источника.
3. Нажмите кнопку **Скачать файлы журналов** → **<Период>**.

Файлы журналов источника собраны, добавлены в ZIP-архив и скачаны на ваш компьютер.

24. О технической поддержке

Гарантийная поддержка доступна для всех владельцев действующих лицензий на PT Email Security в течение периода предоставления обновлений и включает в себя следующий набор услуг.

Предоставление доступа к обновленным версиям продукта

Обновления продукта выпускаются в порядке и в сроки, определяемые Positive Technologies. Positive Technologies предоставляет обновленные версии продукта в течение оплаченного периода получения обновлений, указанного в бланке лицензии приобретенного продукта Positive Technologies.

Positive Technologies не производит установку обновлений продукта в рамках гарантийной поддержки и не несет ответственности за инциденты, возникшие в связи с некорректной или несвоевременной установкой обновлений продукта.

Восстановление работоспособности продукта

Специалист Positive Technologies проводит диагностику заявленного сбоя и предоставляет рекомендации для восстановления работоспособности продукта. Восстановление работоспособности может заключаться в выдаче рекомендаций по установке продукта заново с потенциальной потерей накопленных данных либо в восстановлении версии продукта из доступной резервной копии (резервное копирование должно быть настроено заблаговременно). Positive Technologies не несет ответственности за потерю данных в случае неверно настроенного резервного копирования.

Примечание. Помощь оказывается при условии, что конечным пользователем продукта соблюдены все аппаратные, программные и иные требования и ограничения, описанные в документации к продукту.

Устранение ошибок и дефектов в работе продукта в рамках выпуска обновленных версий

Если в результате диагностики обнаружен дефект или ошибка в работе продукта, Positive Technologies обязуется включить исправление в ближайшие возможные обновления продукта (с учетом релизного цикла продукта, приоритета дефекта или ошибки, сложности требуемых изменений, а также экономической целесообразности исправления). Сроки выпуска обновлений продукта остаются на усмотрение Positive Technologies.

Рассмотрение предложений по доработке продукта

При обращении с предложением по доработке продукта необходимо подробно описать цель такой доработки. Вы можете поделиться рекомендациями по улучшению продукта и оптимизации его функциональности. Positive Technologies обязуется рассмотреть все предложения, однако не принимает на себя обязательств по реализации каких-либо

доработок. Если Positive Technologies принимает решение о доработке продукта, то способы ее реализации остаются на усмотрение Positive Technologies. Заявки принимаются [на портале технической поддержки](#).

Портал технической поддержки

[На портале технической поддержки](#) вы можете круглосуточно создавать и обновлять заявки и читать новости продуктов.

Для получения доступа к portalу технической поддержки нужно создать учетную запись, используя адрес электронной почты в официальном домене вашей организации. Вы можете указать другие адреса электронной почты в качестве дополнительных. Добавьте в профиль название вашей организации и контактный телефон — так нам будет проще с вами связаться.

Поддержка на портале предоставляется на русском и английском языках.

Условия предоставления гарантийной поддержки

Для получения гарантийной поддержки необходимо оставить заявку [на портале технической поддержки](#) и предоставить следующие данные:

- номер лицензии на использование продукта;
- файлы журналов и наборы диагностических данных, которые требуются для анализа;
- снимки экрана.

Positive Technologies не берет на себя обязательств по оказанию услуг гарантийной поддержки в случае вашего отказа предоставить запрашиваемую информацию или отказа от внедрения предоставленных рекомендаций.

Если заказчик не предоставляет необходимую информацию по прошествии 20 календарных дней с момента ее запроса, специалист технической поддержки имеет право закрыть заявку. Оказание услуг может быть возобновлено по вашей инициативе при условии предоставления запрошенной ранее информации.

Услуги по гарантийной поддержке продукта не включают в себя услуги по переустановке продукта, решение проблем с операционной системой, инфраструктурой заказчика или сторонним программным обеспечением.

Заявки могут направлять уполномоченные сотрудники заказчика, владеющего продуктом на законном основании (включая наличие действующей лицензии). Специалисты заказчика должны иметь достаточно знаний и навыков для сбора и предоставления диагностической информации, необходимой для решения заявленной проблемы.

Услуги по гарантийной поддержке оказываются в отношении поддерживаемых версий продукта. Информация о поддерживаемых версиях содержится в «Политике поддержки версий программного обеспечения» и (или) иных информационных материалах, размещенных на официальном веб-сайте Positive Technologies.

Время реакции и приоритизация заявок

При получении заявки ей присваивается регистрационный номер, специалист службы технической поддержки классифицирует ее (присваивает тип и уровень значимости) и выполняет дальнейшие шаги по ее обработке.

Время реакции рассчитывается с момента получения заявки до первичного ответа специалиста технической поддержки с уведомлением о взятии заявки в работу. Время реакции зависит от уровня значимости заявки. Специалист службы технической поддержки оставляет за собой право переопределить уровень значимости в соответствии с приведенными ниже критериями. Указанные сроки являются целевыми, но возможны отклонения от них по объективным причинам.

Таблица 6. Время реакции на заявку

Уровень значимости заявки	Критерии значимости заявки	Время реакции на заявку
Критический	Аварийные сбои, приводящие к невозможности штатной работы продукта (исключая первоначальную установку) либо оказывающие критически значимое влияние на бизнес заказчика	До 4 часов
Высокий	Сбои, проявляющиеся в любых условиях эксплуатации продукта и оказывающие значительное влияние на бизнес заказчика	До 8 часов
Средний	Сбои, проявляющиеся в специфических условиях эксплуатации продукта либо не оказывающие значительного влияния на бизнес заказчика	До 8 часов
Низкий	Вопросы информационного характера либо сбои, не влияющие на эксплуатацию продукта	До 8 часов

Указанные часы относятся к рабочему времени (рабочие дни с 9:00 до 18:00 UTC+3) специалистов технической поддержки. Под рабочим днем понимается любой день за исключением субботы, воскресенья и дней, являющихся официальными нерабочими днями в Российской Федерации.

Обработка и закрытие заявок

По мере рассмотрения заявки и выполнения необходимых действий специалист службы поддержки сообщает вам:

- о ходе диагностики по заявленной проблеме и ее результатах;
- планах выпуска обновленной версии продукта (если требуется для устранения проблемы).

Если по итогам обработки заявки необходимо внести изменения в продукт, Positive Technologies включает работы по исправлению в ближайшее возможное плановое обновление продукта (с учетом релизного цикла продукта, приоритета дефекта или ошибки, сложности требуемых изменений, а также экономической целесообразности исправления). Сроки выпуска обновлений продукта остаются на усмотрение Positive Technologies.

Специалист закрывает заявку, если:

- предоставлены решение или возможность обойти проблему, не влияющие на критически важную функциональность продукта (по усмотрению Positive Technologies);
- диагностирован дефект продукта, собрана техническая информация о дефекте и условиях его воспроизведения, исправление дефекта запланировано к выходу в рамках планового обновления продукта;
- заявленная проблема вызвана программным обеспечением или оборудованием сторонних производителей, на которые не распространяются обязательства Positive Technologies;
- заявленная проблема классифицирована специалистами Positive Technologies как неподдерживаемая.

Примечание. Если продукт приобретался вместе с аппаратной платформой в виде программно-аппаратного комплекса (ПАК), решение заявок, связанных с ограничением или отсутствием работоспособности аппаратных компонентов, происходит согласно условиям и срокам, указанным в гарантийных обязательствах (гарантийных талонах) на такие аппаратные компоненты.

Приложение. Сценарии отказов

Если развернута конфигурация PT Email Security с отказоустойчивым кластером, при выходе из строя любого аппаратного компонента (например, жесткого диска или модуля ОЗУ), физического сервера или при потере сетевого доступа к одному из узлов PT Email Security продукт продолжит обрабатывать задания на проверку файлов в штатном режиме. Однако при возникновении неполадок может быть потеряна часть данных, на короткое время некоторые компоненты могут стать недоступными или может ухудшиться их производительность.

Таблица 7. Сценарии отказов компонентов PT Email Security

Компонент	Следствие отказа		
	Потерянные данные	Недоступность компонентов и функций	Ухудшение производительности
Служба высокой доступности Keeralived	Результаты проверки файлов, которые проверялись на момент отказа	ICAP-сервер, почтовый сервер в режиме зеркалирования, почтовый сервер в режиме фильтрации — 40 секунд	—
Веб-интерфейс	—	Веб-интерфейс — до 5 минут	—
База данных	Завершенные задания	Запись в базу данных — 20 секунд	—
API базы данных	Текущие задания в веб-интерфейсе	Запись в базу данных — 90 секунд	—
Ядро проверки	Часть файлов у трети текущих заданий	—	—
Хранилище файлов	Файлы	—	Модуль поведенческого анализа, скачивание файлов
Модуль поведенческого анализа	—	—	Модуль поведенческого анализа

Глоссарий

Checkme

Служба для проверки объектов по электронной почте. Пользователь может отправить объект или переслать письмо на специальный электронный адрес и получить результат проверки в ответном письме.

Keepalived

Служба, которая обеспечивает доступ к продукту по одному IP-адресу, независимо от того, какой из узлов отказоустойчивого кластера активен.

блокирующий режим

Режим проверки, при котором поступившие на проверку объекты блокируются продуктом до окончания проверки. В зависимости от вынесенного вердикта объект пропускается в информационную систему или удаляется (или помещается в карантин).

источник для проверки

Интерфейс в информационной системе организации, с которого в продукт поступают объекты на проверку.

карантин

Изолированная часть хранилища файлов, позволяющая сохранять заблокированные файлы с угрозами для последующего анализа.

пассивный режим

Режим проверки, при котором поступившие на проверку объекты сразу пропускаются продуктом в информационную систему.

режим зеркалирования

Режим работы почтового сервера, при котором продукт не влияет на почтовый трафик сервера. На проверку в продукт отправляются копии писем.

режим ожидания

Режим проверки, при котором на проверку от источников в продукт поступают копии объектов, а их распространение контролирует пользователь или сторонняя система.

режим фильтрации

Режим работы почтового сервера, при котором продукт может фильтровать почтовый трафик сервера. В зависимости от выбранного режима проверки продукт либо сразу возвращает почтовому серверу отправленное на проверку письмо (пассивный режим), либо блокирует его до окончания проверки (блокирующий режим).



Positive Technologies — один из лидеров в области результативной кибербезопасности. Компания является ведущим разработчиком продуктов, решений и сервисов, позволяющих выявлять и предотвращать кибератаки до того, как они причинят неприемлемый ущерб бизнесу и целым отраслям экономики. Positive Technologies — первая и единственная компания из сферы кибербезопасности на Московской бирже (MOEX: POSI). Количество акционеров превышает 220 тысяч.



Email Security

версия 5.30

Руководство специалиста по
безопасности

© Positive Technologies, 2026.

Настоящий документ является собственностью Positive Technologies и защищен законодательством Российской Федерации и международными соглашениями об авторских правах и интеллектуальной собственности.

Копирование документа либо его фрагментов в любой форме, распространение, в том числе в переводе, а также их передача третьим лицам возможны только с письменного разрешения Positive Technologies.

Документ может быть изменен без предварительного уведомления.

Товарные знаки, использованные в тексте, приведены исключительно в информационных целях, исключительные права на них принадлежат соответствующим правообладателям.

Дата редакции документа: 06.02.2026

Содержание

1.	Об этом документе.....	5
1.1.	Условные обозначения.....	5
1.2.	Другие источники информации о PT Email Security.....	6
2.	О PT Email Security.....	7
3.	Требования к рабочим станциям.....	9
4.	Анонимная проверка объектов.....	10
5.	Проверка объектов по электронной почте.....	11
6.	Вход в PT Email Security.....	12
7.	Интерфейс PT Email Security.....	13
8.	Мониторинг работы PT Email Security.....	16
9.	Проверка объектов.....	22
9.1.	Алгоритм и особенности проверки объектов.....	24
9.2.	Проверка объектов через веб-интерфейс.....	28
9.3.	Поведенческий анализ в интерактивном режиме.....	28
9.4.	Параметры проверки объектов.....	29
9.5.	Управление очередью файлов на поведенческий анализ.....	35
10.	Работа с результатами проверки.....	40
10.1.	Поиск по заданиям.....	40
10.2.	Поиск по объектам.....	45
10.3.	Работа с карточкой задания.....	51
10.4.	Работа с карточкой поведенческого анализа.....	59
10.5.	Просмотр очереди обработки писем MTA.....	64
10.6.	Просмотр событий по письмам.....	66
10.7.	Работа с письмами в карантине.....	68
10.8.	Скачивание файлов из хранилища.....	73
11.	Настройка средств проверки.....	79
11.1.	Настройка средств проверки Positive Technologies.....	79
11.2.	Просмотр доступных антивирусов.....	82
11.3.	Настройка поведенческого анализа.....	83
11.4.	Работа с образами VM.....	88
11.5.	Работа с черным и белым списками.....	92
11.6.	Работа с пользовательскими YARA-правилами.....	95
12.	Настройка основных параметров PT Email Security.....	100
13.	Просмотр токенов доступа.....	103
14.	Работа с источниками.....	104
14.1.	Настройка параметров проверки объектов от источников.....	107
14.2.	Параметры проверки объектов от источников.....	109
14.3.	Настройка правил приема писем для почтового шлюза безопасности.....	118
14.4.	Настройка обработки писем по правилам.....	123
14.5.	Настройка блокирующего режима проверки писем.....	129
14.6.	Настройка блокирующего режима проверки файлов.....	132
14.7.	Настройка пользовательских правил определения файлов с угрозами.....	133
14.8.	Настройка проверки архивов.....	136

14.9.	Настройка проверки ссылок.....	136
14.10.	Настройка пользовательских правил определения ссылок с угрозами.....	138
14.11.	Отключение сохранения файлов без угроз в хранилище.....	140
14.12.	Настройка правил поведенческого анализа	140
15.	Просмотр конфигурации PT Email Security.....	143
16.	Мониторинг системных ресурсов в Grafana	147
17.	О технической поддержке.....	151
Приложение А. Типы файлов, отправляемых на поведенческий анализ.....		155
Приложение Б. Прикладные протоколы, поддерживаемые PT Email Security при поведенческом анализе файлов		157
Приложение В. Базовые образы VM.....		161
Приложение Г. Метки объектов		164
Приложение Д. Синтаксис языка запросов QL.....		171
Д.1.	Поля QL-запросов	174
Д.2.	Типы вредоносного ПО	198
Глоссарий.....		206

1. Об этом документе

Руководство специалиста по безопасности содержит пошаговые инструкции и справочную информацию об использовании Positive Technologies Email Security (далее также — PT Email Security) для управления инцидентами информационной безопасности. Руководство не содержит инструкций по установке и администрированию PT Email Security.

Руководство адресовано руководителям и специалистам, ответственным за обеспечение информационной безопасности, контроль и расследование инцидентов.

Комплект документации PT Email Security включает в себя следующие документы:

- Этот документ.
- Руководство по внедрению — содержит информацию для внедрения продукта в инфраструктуре организации: от описания типовых конфигураций до инструкций по установке и первоначальной настройке продукта.
- Руководство администратора — содержит справочную информацию и инструкции по настройке и администрированию продукта.
- Руководство пользователя — содержит инструкции по отправке файлов на проверку через интерфейс продукта или по электронной почте и просмотру результатов проверки.
- Руководство разработчика — содержит информацию для интеграции PT Email Security со сторонними системами.

В этом разделе

[Условные обозначения \(см. раздел 1.1\)](#)

[Другие источники информации о PT Email Security \(см. раздел 1.2\)](#)

1.1. Условные обозначения

В документе приняты условные обозначения.

Таблица 1. Условные обозначения

Пример	Описание
Внимание! При выключении модуля снижается уровень защищенности сети	Предупреждения. Содержат информацию о действиях или событиях, которые могут иметь нежелательные последствия
Примечание. Вы можете создать дополнительные отчеты	Примечания. Содержат советы, описания важных частных случаев, дополнительную или справочную информацию, которая может быть полезна при работе с продуктом
► Чтобы открыть файл:	Начало инструкции выделено специальным значком

Пример	Описание
Нажмите OK	Названия элементов интерфейса (например, кнопок, полей, пунктов меню) выделены полужирным шрифтом
Выполните команду <code>Stop-Service</code>	Текст командной строки, примеры кода, прочие данные, которые нужно ввести с клавиатуры, выделены специальным шрифтом. Также выделены специальным шрифтом имена файлов и пути к файлам и папкам
Ctrl+Alt+Delete	Комбинация клавиш. Чтобы использовать комбинацию, клавиши нужно нажимать одновременно
<Название программы>	Переменные заключены в угловые скобки

1.2. Другие источники информации о PT Email Security

Вы можете найти дополнительную информацию о PT Email Security [на портале технической поддержки](#).

Портал содержит статьи базы знаний, новости обновлений продуктов Positive Technologies, ответы на часто задаваемые вопросы пользователей. Для доступа к базе знаний и всем новостям нужно создать на портале учетную запись.

Если вы не нашли нужную информацию или решение проблемы самостоятельно, обратитесь [в службу технической поддержки \(см. раздел 17\)](#).

2. О PT Email Security

Positive Technologies Email Security (PT Email Security) — система многоуровневой защиты от угроз электронной почты с функциями почтового шлюза и почтового транспортного агента. В системе применяются различные средства статического и динамического анализа объектов, включая антифишинг- и антиспам-проверку, антивирусное сканирование, репутационный, ретроспективный и поведенческий анализ.

PT Email Security предназначен для выявления вредоносных объектов, предотвращения их проникновения и распространения в IT-инфраструктуре организации. Многоуровневая проверка позволяет повысить вероятность обнаружения объектов с угрозами.

PT Email Security может использоваться специалистами по информационной безопасности, администраторами и аналитиками SOC для анализа подозрительных объектов и расследования инцидентов информационной безопасности.

PT Email Security предоставляет следующие основные возможности:

- Инструменты для работы с письмами:
 - Почтовый шлюз безопасности с фильтрацией подключений.
 - Встроенный почтовый транспортный агент.
 - Обработка писем в зависимости от отправителя и получателей.
 - Обезвреживание писем с угрозами.
 - Карантин для подозрительных писем.
- Многоуровневая проверка объектов с использованием методов статического и динамического анализа:
 - Поведенческий анализ файлов в различных операционных системах.
 - Антивирусная проверка файлов.
 - Проверка файлов по YARA-правилам, разработанным специалистами экспертного центра Positive Technologies.
 - Проверка файлов и ссылок по индикаторам компрометации.
 - Антифишинг- и антиспам-проверка писем.
 - Проверка адресов в письмах по спискам DNS-блокировок.
 - Ретроспективный анализ файлов в хранилище.
- Настраиваемые пользователем средства проверки:
 - Черный и белый списки файлов.
 - Проверка файлов по пользовательским YARA-правилам.
 - Пользовательские правила определения файлов и ссылок с угрозами.

- Экспертные инструменты для проверки объектов и расследования инцидентов:
 - Гибкий поиск заданий и объектов с использованием языка запросов QL.
 - Проверка объектов по базам VirusTotal и PT IoC Portal.
 - Поведенческий анализ файлов в интерактивном режиме.
 - Диаграммы поведенческого анализа.
- Быстрая проверка объектов через веб-интерфейс или по электронной почте.
- Поточковая проверка объектов, поступающих из различных источников:
 - Почтовый трафик серверов электронной почты с возможностью блокировки писем с угрозами.
 - Объекты от ICAP-клиентов с возможностью блокировки объектов с угрозами.
 - Объекты из файловых хранилищ и файловых шлюзов.
 - Объекты, передаваемые через публичный API PT Email Security.
- Интеграция с продуктами Positive Technologies:
 - MaxPatrol EDR.
 - MaxPatrol SIEM.
 - PT AF.
 - PT ISIM.
 - PT NAD.
 - PT NGFW.
 - PT Threat Analyzer.

PT Email Security также предоставляет дополнительные возможности:

- Мониторинг проверки объектов и обнаруженных угроз.
- Отправка почтовых уведомлений об угрозах.
- Управление очередью файлов, направляемых на поведенческий анализ.
- Управление приоритетами источников и типов файлов при поведенческом анализе.
- Формирование отчетов по заданиям и проверенным объектам.
- Скачивание проверенных файлов из хранилища.
- Мониторинг работы PT Email Security в Grafana с возможностью отправки почтовых уведомлений.

3. Требования к рабочим станциям

К рабочим станциям специалистов по безопасности, выдвигаются следующие аппаратные и программные требования:

- Разрешение монитора — Full HD (не менее 1920 × 1080 пикселей).
- Браузер — Google Chrome версии 140, Microsoft Edge 140, Mozilla Firefox 142, Yandex Browser 25.8 или более новых версий.
- На узле должны быть разрешены исходящие подключения к портам TCP 80, 443, 3334, 8703, 8704.
- Если на узле установлен антивирус:
 - В исключения антивируса должны быть добавлены правила, которые разрешают доступ к основному узлу PT Email Security и используемым прокси-серверам по протоколам HTTP и HTTPS.
 - В PT Email Security должен быть установлен пользовательский SSL-сертификат, выпущенный доверенным центром сертификации.

4. Анонимная проверка объектов

Вы можете анонимно проверять по одному файлу или ссылке через веб-интерфейс PT Email Security, не выполняя аутентификацию.

Примечание. Анонимная проверка должна быть включена администратором PT Email Security в основных параметрах системы.

► Чтобы проверить объект:

1. В адресной строке браузера введите адрес веб-интерфейса PT Email Security.
Откроется страница анонимной проверки объектов.
2. Выберите тип объекта.
3. Если вы выбрали **Файл**, перетащите файл в область загрузки на странице или загрузите его по ссылке **выберите**.
4. Если вы выбрали **Ссылка**, введите ссылку.
5. Если вы хотите проверить архив, защищенный нестандартным паролем, в поле **Пароли для архива** укажите этот пароль.
6. Нажмите кнопку **Проверить**.

Откроется карточка задания на проверку объекта.

Примечание. Вы можете вернуться на страницу анонимной проверки, нажав < .

5. Проверка объектов по электронной почте

Если в вашей организации настроена служба Checkme, вы можете отправлять файлы и ссылки на проверку в PT Email Security по электронной почте. Объекты необходимо отправлять письмом на специальный адрес электронной почты службы Checkme. Также на этот адрес вы можете отправлять на проверку письма, полученные вами от других адресатов. Результаты проверки придут вам в ответном письме. Из ответного письма вы также сможете перейти в веб-интерфейс PT Email Security, чтобы посмотреть более подробную информацию о проверке.

Примечание. Отправленные по электронной почте объекты проверяются с параметрами проверки источника, добавленного для службы Checkme.

► Чтобы отправить объекты на проверку по электронной почте:

1. В вашей почтовой программе создайте новое письмо:
 - В поле получателя введите адрес электронной почты службы Checkme.
Внимание! Не добавляйте других адресатов.
 - Прикрепите к письму файлы для проверки.
 - В тексте письма введите ссылки для проверки.
 - Если вы отправляете зашифрованный архив, в тексте письма введите пароль (если паролей несколько, по одному в строке).
2. Отправьте письмо.

6. Вход в PT Email Security

Вход в PT Email Security выполняется с помощью компонента PT MC, который обеспечивает единый механизм входа в продукты Positive Technologies.

Для входа в PT Email Security вам понадобится адрес веб-интерфейса PT Email Security и данные учетной записи.

► Чтобы войти в PT Email Security:

1. В адресной строке браузера введите адрес веб-интерфейса PT Email Security и нажмите клавишу Enter.

Откроется страница входа в PT Email Security или страница для анонимной проверки объектов.

2. Нажмите кнопку **Войти**.

Откроется страница входа в PT MC.

3. Если вы используете доменную учетную запись, выберите вкладку **LDAP**.

4. Введите данные учетной записи.

5. Нажмите кнопку **Войти**.

Откроется веб-интерфейс PT Email Security.

7. Интерфейс PT Email Security

Работа с PT Email Security выполняется через веб-интерфейс. Все передаваемые при работе данные защищаются при помощи HTTPS с использованием SSL-сертификата. Сертификат может быть как самоподписанным, так и выданным официальным центром сертификации.

Главное меню

Для доступа пользователей к страницам веб-интерфейса и основным функциям PT Email Security используется главное меню. В главном меню расположены следующие элементы управления.

 — кнопка для перехода между приложениями Positive Technologies, которые зарегистрированы в сервисе управления пользователями и доступом PT MC.

Разделы для перехода к страницам веб-интерфейса:

- **Сводка** — для просмотра сводной информации о выполненных заданиях и проверенных файлах.
- **Задания** — для работы с заданиями на проверку объектов.
- **Объекты** — для работы с объектами в хранилище.
- **Письма** — содержит пункты для перехода к следующим страницам:
 - **Очередь обработки МТА** — для просмотра очереди обработки писем почтовым транспортным агентом.
 - **События по письмам** — для просмотра событий, связанных с письмами.
 - **Карантин** — для работы с письмами в карантине.
- **Средства проверки** — содержит пункты для перехода к следующим страницам:
 - **Экспертиза РТ** — для работы со средствами проверки, которые разработаны специалистами Positive Technologies.
 - **Антивирусы** — для работы с антивирусами сторонних разработчиков, которые используются при проверке файлов.
 - **Поведенческий анализ** — содержит пункты для перехода к страницам управления очередью файлов на поведенческий анализ, настройки приоритета файлов, времени хранения результатов поведенческого анализа, а также подраздел с пунктами для перехода на страницы работы с образами виртуальных машин, используемых при поведенческом анализе файлов.
 - **Черный список** — для работы с хеш-суммами безусловно опасных файлов.
 - **Белый список** — для работы с хеш-суммами безусловно безопасных файлов.
 - **Пользовательские правила** — для работы со средством проверки объектов по пользовательским YARA-правилам.

- **Источники** — для работы с источниками, от которых поступают объекты на проверку.
- **Система** — содержит пункты для перехода к следующим страницам:
 - **Основные параметры** — для настройки основных параметров работы PT Email Security.
 - **Токены доступа** — для работы с токенами для доступа к PT Email Security через публичный API.

Проверить объекты — кнопка для проверки объектов через веб-интерфейс.

Также в главном меню расположены значки:

 — для просмотра уведомлений о проверке объектов, отправленных вами через интерфейс. На значке отображается количество проверенных объектов. По ссылке в уведомлении вы можете открыть карточку задания, в котором проверен объект.

 — для просмотра уведомлений о работе компонентов PT Email Security и доступных обновлениях. На значке отображается количество новых уведомлений. При нажатии на значок вы можете:

- Посмотреть версию PT Email Security.
- Скачать файлы журналов PT Email Security.
- Перейти на сайт технической поддержки Positive Technologies.

 — для просмотра логина, под которым вы вошли в PT Email Security. При нажатии на значок вы можете:

- Сменить тему оформления и язык интерфейса.
- Выйти из PT Email Security.

Смена языка и темы оформления интерфейса

Интерфейс PT Email Security доступен на русском и английском языках в светлой и темной темах оформления. По умолчанию выбраны русский язык и светлая тема.

- ▶ Чтобы сменить язык интерфейса,

в главном меню выберите  → **Язык** → **<Название языка>**.

- ▶ Чтобы сменить тему интерфейса,

в главном меню выберите  → **Тема** → **<Название темы>**.

Примечание. Для выбора темы, соответствующей оформлению интерфейса ОС, вы можете выбрать **Системная**.

Аудит действий пользователей

В PT Email Security реализован аудит действий пользователей. Регистрируются события безопасности, связанные со следующими действиями пользователей:

- просмотр заданий;
- скачивание результатов проверки и файлов из хранилища;
- очистка очереди файлов на поведенческий анализ;
- просмотр и выпуск писем из карантина;
- изменение параметров проверки источников;
- изменение параметров средств проверки Positive Technologies;
- работа с черным и белым списками (очистка, скачивание);
- работа с записями в черном и белом списках (добавление, удаление, перемещение между списками, добавление комментариев);
- работа с образами виртуальных машин (добавление, удаление и скачивание);
- скачивание файлов журналов;
- изменение основных параметров PT Email Security.

Все зарегистрированные события отображаются в журнале действий PT MC.

8. Мониторинг работы PT Email Security

Для мониторинга работы PT Email Security и просмотра информации о выполненных заданиях предназначена страница **Сводка**. Страница открывается сразу после входа в PT Email Security или при выборе в главном меню раздела **Сводка**.

В верхней части страницы расположены:

- Кнопка для выбора периода времени. Данные на виджетах отображаются для указанного вами периода.
- Кнопка ⓘ для просмотра списка выполненных ранее QL-запросов.
- Поле для ввода [QL-запроса \(см. приложение Д\)](#). Если вы ввели запрос, на виджетах отображаются данные о заданиях и объектах, удовлетворяющих запросу.

Примечание. По кнопке ✕ вы можете очистить поле для ввода QL-запроса.

- Кнопки ↻ и ⚙ для обновления информации на виджетах и настройки автоматического обновления.

В рабочей области страницы расположены виджеты с данными.

Виджет с распределением данных по времени

Виджет предназначен для просмотра динамики изменения ряда величин, связанных с работой PT Email Security, в зависимости от времени. Например, с помощью виджета вы можете отслеживать изменение количества заданий на проверку, созданных в единицу времени. На виджете отображаются данные за указанный вами период времени, которые соответствуют указанному вами запросу.



Рисунок 1. Виджет с распределением данных по времени

В верхней части виджета расположен раскрывающийся список для выбора отслеживаемых величин. Для выбранных величин в списке отображаются их суммарные значения, например общее количество заданий за выбранный период. Доступны графики для следующих величин:

- **Заданий** — количество созданных заданий на проверку.

Примечание. При наведении курсора на виджет появляется окно с точными значениями выбранных величин в соответствующий момент времени.

- **Заданий с опасными файлами** — количество заданий, в которых обнаружены опасные файлы.
- **Заданий с потенциально опасными файлами** — количество заданий, в которых обнаружены потенциально опасные файлы.
- **Файлов** — количество проверенных файлов без учета файлов, полученных при поведенческом анализе (AMSI-скриптов, дампов памяти и dropped файлов).
- **Ссылок** — количество проверенных ссылок.
- **Артефактов ПА** — количество файлов, полученных при поведенческом анализе (AMSI-скриптов, дампов памяти и dropped файлов).
- **Файлов с ПА** — количество файлов, проверенных методом поведенческого анализа.
- **Запусков ПА** — общее количество запусков поведенческого анализа файлов.
- **Неудачных запусков ПА** — количество запусков поведенческого анализа файлов, при которых проверка была выполнена частично или с ошибками.

Виджеты с распределением данных по вердиктам и тактикам MITRE ATT&CK

На виджетах отображаются данные за указанный вами период времени, которые соответствуют указанному вами запросу.

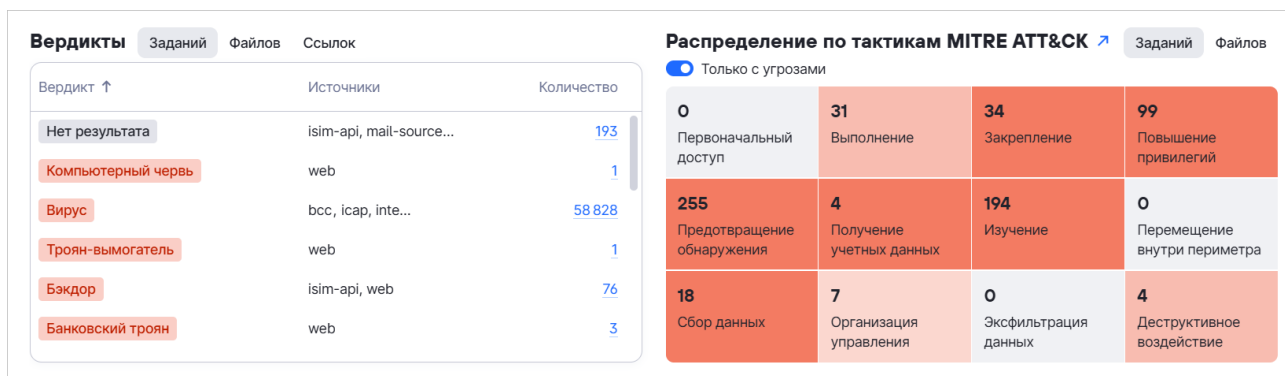


Рисунок 2. Виджеты с распределением данных по вердиктам и тактикам MITRE ATT&CK

Виджет **Вердикты** предназначен для просмотра распределения количества заданий, проверенных файлов (с учетом артефактов поведенческого анализа) или ссылок по вынесенным для них вердиктам.

В верхней части виджета с помощью кнопок **Заданий**, **Файлов** и **Ссылок** вы можете выбрать данные, для которых в таблице на виджете будет отображаться распределение по вердиктам. Таблица содержит следующие столбцы:

- **Вердикт** — в столбце указан вердикт, вынесенный по заданию или объекту.
- **Источники** — в столбце указаны источники, от которых поступали задания или объекты с такими вердиктами.
- **Количество** — в столбце указано количество заданий или объектов с вердиктом. По ссылкам вы можете открыть страницу со списком заданий или объектов с этим вердиктом.

Примечание. Нажимая на заголовки столбцов **Вердикт** и **Количество**, вы можете настроить сортировку в таблице.

Виджет **Распределение по тактикам MITRE ATT&CK** предназначен для просмотра распределения количества проверенных заданий или файлов (с учетом артефактов поведенческого анализа) по тактикам и техникам MITRE ATT&CK. Учитываются только файлы, которые проверены методом поведенческого анализа и в которых обнаружено подозрительное поведение, или задания с такими файлами.

Примечание. По ссылке в заголовке виджета вы можете перейти на портал mitre.ptsecurity.com.

В верхней части виджета с помощью кнопок **Заданий** и **Файлов** вы можете выбрать данные, для которых на виджете будет отображаться распределение по тактикам MITRE ATT&CK. С помощью выключателя **Только с угрозами** вы можете выбрать, какие задания (файлы) с обнаруженным подозрительным поведением нужно учитывать: все или только те, для которых вынесен вердикт о наличии угрозы. В каждой ячейке с названием тактики указывается количество заданий (файлов), в которых при поведенческом анализе было обнаружено подозрительное поведение с использованием одной из техник, относящихся к этой тактике. Цвет ячейки указывает максимальный рейтинг опасности обнаруженных техник: чем насыщенней цвет, тем выше опасность. При нажатии на ячейку открывается окно с информацией о техниках.

Повышение привилегий ×			
ID	Техника	Рейтинг ↓	Заданий
T1055	Внедрение кода в процессы ↗	10/10	2
T1547	Автозапуск при загрузке или входе в систему...	9/10	7
T1548	Обход механизмов контроля привилегий ↗	5/10	8

Рисунок 3. Окно с информацией об обнаруженных техниках из тактики «Повышение привилегий»

Окно содержит таблицу со следующими столбцами:

- **ID** — в столбце указан идентификатор техники согласно матрице MITRE ATT&CK.
- **Техника** — в столбце указано название техники. По ссылке в названии вы можете перейти на сайт attack.mitre.org с подробным описанием техники.
- **Рейтинг** — в столбце указан рейтинг опасности техники по оценке специалистов Positive Technologies.
- **Заданий** или **Файлов** — в столбце указано количество заданий или файлов, в которых обнаружено использование техники. По ссылке вы можете открыть страницу со списком таких заданий или файлов.

Примечание. Нажимая на заголовки столбцов **ID**, **Рейтинг**, **Заданий** или **Файлов**, вы можете настроить сортировку в таблице.

Виджеты с распределением данных по различным параметрам

Виджеты предназначены для просмотра распределения количества проверенных заданий, файлов (с учетом артефактов поведенческого анализа) или ссылок по различным параметрам. На виджетах отображаются данные за указанный вами период времени, которые соответствуют указанному вами запросу.

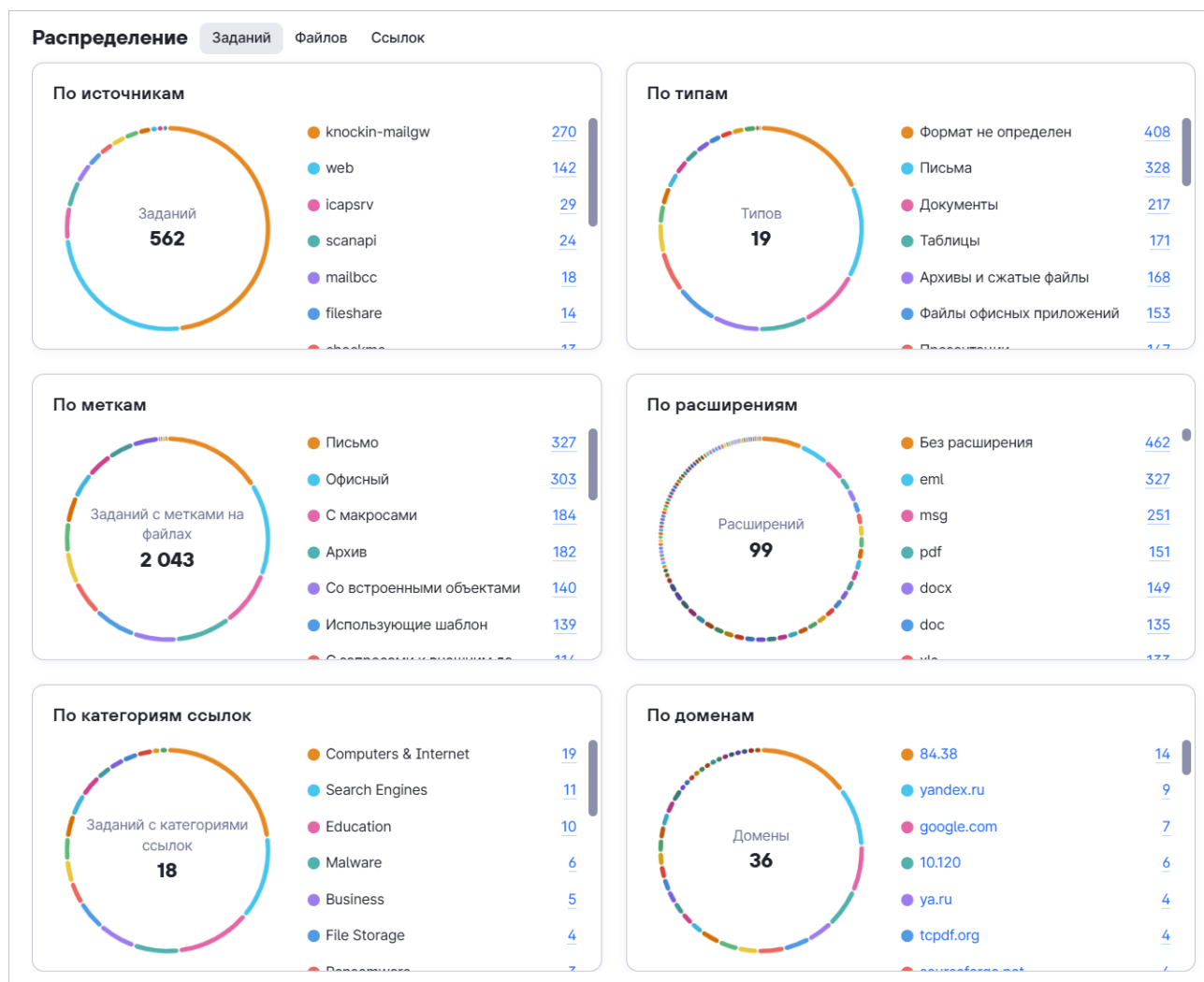


Рисунок 4. Виджеты с распределением данных по различным параметрам

В верхней части блока виджетов с помощью кнопок **Заданий**, **Файлов** и **Ссылок** вы можете выбрать данные для отображения на виджетах. На каждом виджете расположена круговая диаграмма, которая показывает долю каждой составляющей в общем количестве данных. В правой части каждого виджета расположен список, в котором указано количество заданий или объектов, относящихся к каждой составляющей. По ссылкам вы можете открыть страницу со списком заданий или объектов для каждой составляющей.

Доступны следующие виджеты для просмотра распределений данных:

- **По источникам** — распределение данных по источникам объектов. В списке указаны названия добавленных источников и количество поступивших от них заданий, файлов или ссылок. В центре круговой диаграммы указано общее количество поступивших заданий или объектов.
- **По типам** — распределение данных по типам проверенных файлов. В списке указаны названия типов файлов и количество заданий на проверку файлов этого типа. Для файлов указывается количество проверенных файлов этого типа, для ссылок — количество проверенных ссылок на файлы этого типа. В центре круговой диаграммы указано общее количество различных типов файлов.
- **По меткам** — распределение данных по установленным для файлов меткам. В списке указаны названия меток и количество заданий на проверку файлов с такими метками. Для файлов указывается количество проверенных файлов с такими метками, для ссылок — количество проверенных ссылок на файлы с такими метками. В центре круговой диаграммы указано общее количество заданий с метками на файлах или общее количество файлов с метками.
- **По расширениям** — распределение данных по расширениям файлов. В списке указаны расширения файлов и количество заданий на проверку файлов с такими расширениями. Для файлов указывается количество проверенных файлов с такими расширениями, для ссылок — количество проверенных ссылок на файлы с такими расширениями. В центре круговой диаграммы указано количество различных расширений файлов.
- **По категориям ссылок** — распределение данных по категориям ссылок. Виджет доступен только для заданий и ссылок. В списке указаны названия категорий и количество заданий на проверку ссылок с такими категориями. Для ссылок указывается количество проверенных ссылок с такими категориями. В центре круговой диаграммы указано общее количество заданий с категориями ссылок или общее количество различных категорий ссылок.
- **По доменам** — распределение данных по доменам второго уровня в ссылках. Виджет доступен только для заданий и ссылок. В списке указаны имена доменов второго уровня и количество заданий на проверку ссылок с такими доменами. Для ссылок указывается количество проверенных ссылок с такими доменами. По ссылке в имени домена вы можете перейти к аналогичному распределению данных по доменам третьего уровня. В центре круговой диаграммы указано количество различных доменов.

9. Проверка объектов

Для выявления угроз в отправленных на проверку объектах PT Email Security использует статические и динамические методы анализа.

Статический анализ

К статическому анализу относятся следующие методы проверки:

- **Антивирусное сканирование файлов.** Антивирусное сканирование выполняется с использованием антивирусов сторонних разработчиков. Проверка позволяет выявлять известные угрозы, включая вирусы, трояны, шпионское ПО, рекламное ПО и другие виды угроз, на основе сигнатурного и эвристического анализа. Использование антивирусных решений от нескольких независимых разработчиков позволяет снизить вероятность пропуска вредоносных объектов.
- **Экспертная проверка файлов.** Такая проверка выполняется с использованием YARA-правил, разработанных специалистами экспертного центра Positive Technologies. Эти правила позволяют выявлять файлы с угрозами, анализируя их содержимое на наличие характерных сигнатур, структурных особенностей и других признаков, присущих вредоносному ПО. Проверка выполняется с помощью средства проверки PT ESC.
- **Проверка файлов по пользовательским YARA-правилам.** Такая проверка выполняется с использованием правил, созданных специалистами по информационной безопасности вашей организации. Пользовательские YARA-правила позволяют обнаруживать угрозы, не детектируемые другими средствами проверки, и оперативно адаптировать PT Email Security под актуальные задачи информационной безопасности.
- **Проверка файлов по черному и белому спискам.** Во время этой проверки хеш-суммы файлов сопоставляются с хеш-суммами вредоносных и доверенных объектов в черном и белом списках. Эти списки могут формироваться специалистами по безопасности вашей организации или загружаться извне.
- **Проверка файлов и ссылок по индикаторам компрометации.** При проверке по индикаторам компрометации (IoC) файлы и ссылки сопоставляются с известными признаками подозрительной или вредоносной активности. Для файлов такими индикаторами могут быть хеш-суммы, для ссылок — URL, IP-адреса и имена доменов. Проверка выполняется с помощью средства проверки PT IoC.
- **Антифишинг- и антиспам-проверка писем.** Позволяет выявлять признаки спама в письмах на основе анализа заголовков и содержимого, включая маршрутизацию, тему, адреса отправителя и получателя. Признаки фишинга выявляются на основе анализа URL-ссылок, содержащихся в письмах, и параметров связанных веб-страниц. Проверка выполняется с помощью средства обнаружения угроз в почте PT Anti-Phishing and Anti-Spam.
- **Проверка адресов в письмах по DNSBL.** В ходе проверки IP-адреса и имена доменов, указанные в заголовках писем и обнаруженные в ссылках и адресах отправителей, сопоставляются с записями в списках DNS-блокировок (DNS-based blackhole list). Такие

списки содержат сведения об IP-адресах и доменных именах, которые связаны с рассылкой спама, фишинговыми атаками и распространением вредоносного ПО. Это позволяет выявлять нежелательные и потенциально опасные письма на основе репутационной информации об источниках их доставки. Проверка выполняется с помощью средства обнаружения угроз в почте PT Anti-Phishing and Anti-Spam.

- **Ретроспективный анализ файлов.** Ретроспективный анализ подразумевает регулярную повторную проверку файлов из хранилища. В ходе проверки используются обновленные антивирусные базы и актуальные базы знаний других средств проверки. Это позволяет выявлять новые угрозы, которые не были обнаружены при первоначальной проверке.

Динамический анализ

К динамическому анализу относятся следующие методы проверки:

- **Поведенческий анализ файлов.** Поведенческий анализ позволяет выявлять вредоносное ПО за счет изучения активности файлов в контролируемой среде. Для этого файл запускается в изолированной ОС, развернутой в виртуальной машине, что предотвращает возможное воздействие на реальную систему. Образ ОС может содержать специальные файлы-приманки, которые выглядят как привлекательная мишень для вредоносного ПО. В ходе анализа PT Email Security имитирует действия пользователя, чтобы спровоцировать выполнение вредоносной активности.

Для повышения эффективности поведенческого анализа в PT Email Security реализован механизм Anti-Evasion, предназначенный для противодействия техникам уклонения от анализа в контролируемой среде. Механизм предотвращает распознавание вредоносным ПО факта поведенческого анализа за счет контроля и маскировки признаков виртуализации, анализа окружения и пользовательской активности, что повышает вероятность активации вредоносного ПО и проявления его вредоносного поведения.

В ходе анализа PT Email Security отслеживает активность файла, включая сетевые соединения, изменения реестра и параметров системы, запуск процессов, а также создание, изменение и удаление файлов. Признаки опасного и потенциально опасного поведения определяются с помощью правил, разработанных специалистами экспертного центра Positive Technologies. Все файлы и артефакты, полученные в ходе анализа, сохраняются в хранилище и дополнительно проверяются методами статического анализа.

- **Анализ файлов с использованием машинного обучения.** Для выявления аномального поведения файлов применяется предобученная модель, разработанная специалистами экспертного центра Positive Technologies. Модель обучена на обширном наборе данных, содержащем как безопасные, так и вредоносные файлы. Это позволяет не только обнаруживать известные угрозы, но и выявлять новые атаки, анализируя отклонения в поведении файла от типичных шаблонов. Анализ выполняется с помощью средства проверки PT ML.

- **Анализ сетевых пакетов.** В ходе поведенческого анализа файла может возникать сетевой трафик между гостевой ОС и внешними сетевыми ресурсами. Для выявления сетевых атак PT Email Security перехватывает сетевые пакеты в трафике и проверяет их с помощью правил, разработанных специалистами экспертного центра Positive Technologies. Анализ выполняется с помощью средства проверки PT DPI.
- **Анализ ссылок.** Предусмотрены простой и расширенный способы проверки ссылок. В обоих случаях контент по ссылкам скачивается с помощью HTTP/HTTPS-клиента. При расширенном способе проверки, если контент имеет формат HTML, после скачивания формируется полноценная веб-страница: загружаются все связанные ресурсы и выполняются сценарии JavaScript. Это позволяет выявлять динамически создаваемые элементы и потенциально вредоносные сценарии. Скачивание контента выполняется с помощью средства проверки PT Crawler. Весь скачанный контент сохраняется в хранилище в виде файлов и проверяется методами статического анализа.

В этом разделе

[Алгоритм и особенности проверки объектов \(см. раздел 9.1\)](#)

[Проверка объектов через веб-интерфейс \(см. раздел 9.2\)](#)

[Поведенческий анализ в интерактивном режиме \(см. раздел 9.3\)](#)

[Параметры проверки объектов \(см. раздел 9.4\)](#)

[Управление очередью файлов на поведенческий анализ \(см. раздел 9.5\)](#)

9.1. Алгоритм и особенности проверки объектов

Проверка объектов в PT Email Security выполняется согласно следующему алгоритму:

1. Объект поступает на проверку в PT Email Security от одного из настроенных источников или через веб-интерфейс. Для объекта создается задание на проверку и карточка задания. В карточку задания добавляется карточка исходного объекта.
2. Выполняются определение типа объекта и выделение дочерних объектов:
 - Если объект является письмом, из него выделяются тело письма, файлы вложений, выполняется поиск ссылок и скачивание файлов по этим ссылкам.
 - Если объект является архивом, выполняется декомпрессия или распаковка файлов. Для зашифрованных архивов выполняется подбор пароля.
 - Если объект является ссылкой, скачивается контент по этой ссылке.

В карточку задания добавляются отдельные карточки для объектов, связанных с исходным объектом.

3. Собираются данные об объектах задания и заносятся в карточки объектов. Например, для файла указываются хеш-суммы (MD5, SHA-1, SHA-256 и SSDEEP), размер и MIME-тип.

4. Каждый объект задания проверяется с помощью различных методов проверки в соответствии с заданными параметрами проверки, результаты проверок заносятся в карточку объекта. На основании результатов проверок принимается решение о наличии или отсутствии угрозы в объекте — выносится вердикт по объекту.
5. На основании вердиктов по отдельным объектам выносится вердикт о наличии или отсутствии угрозы в исходном объекте, поступившем на проверку.
6. Файлы задания сохраняются в хранилище файлов. Извлеченные из архивов файлы и вложения электронных писем сохраняются в хранилище как отдельные файлы. Если файл имеет размер больше 1 ГБ или занимает больше 1% от объема хранилища, он удаляется.
7. Если для источника настроен блокирующий режим работы, в зависимости от вердикта проверенный файл или электронное письмо пропускается в информационную систему или блокируется.

Проверка архивов и сжатых файлов

В ходе проверки PT Email Security извлекает вложенные файлы из архивов и выполняет декомпрессию сжатых файлов. Все полученные при этом файлы проверяются.

Примечание. По умолчанию не распаковываются архивы и сжатые файлы, поступающие на проверку от источников с типами «ICAP-сервер» и «PT NAD».

Если архив содержит вложенные архивы, PT Email Security также извлекает и проверяет вложенные в них файлы. По умолчанию архивы распаковываются до второго уровня вложенности. Архивы следующих уровней вложенности не распаковываются и проверяются как простые файлы. Вы можете изменить глубину распаковки архивов в параметрах проверки.

Если архив защищен паролем, PT Email Security выполняет подбор пароля для распаковки архива. Используются пароли, указанные в параметрах проверки, и пароли из списка стандартных паролей. Архивы, для которых не удалось подобрать пароль, проверяются как простые файлы.

Проверка электронных писем

В ходе проверки электронных писем PT Email Security выделяет из них почтовые заголовки, тело письма, и вложенные файлы. Из тела письма в формате HTML, RTF и TXT извлекаются и проверяются ссылки.

Если в теле письма или во вложенном файле есть изображение с QR-кодом, PT Email Security извлекает ссылку из QR-кода и проверяет ее. Ссылка извлекается из QR-кода, если изображение содержится в теле письма формата HTML (и закодировано в формате Base64) или находится во вложенном файле формата BMP, EXR, GIF, ICO, JPEG, PNG, PNM, QOI, TIFF или WEBP.

Если к письму приложен архив, защищенный паролем, или тело письма содержит ссылку на такой архив, PT Email Security выполняет поиск пароля для распаковки архива в теле письма.

Проверка ссылок

PT Email Security проверяет ссылки, отправленные через веб-интерфейс и извлеченные из других объектов. Все ссылки проверяются по индикаторам компрометации. Кроме того, PT Email Security может скачивать файлы по ссылкам и проверять их.

Таблица 2. Извлечение и проверка дочерних объектов

Тип	Формат	Примечание
Файлы данных		
Архивы ¹	7Z, ACE, ARJ, CPIO, LZH, RAR, TAR, ZIP	Извлекаются и проверяются файлы из архивов, в том числе вложенных
Сжатые файлы	BZ2 (метод сжатия bzip2), GZ ¹ (метод сжатия gzip), LZ ¹ , LZIP ¹ (.lz), LZMA ¹ (.lzma), LZMA2 (.xz), XZ ¹ , Z ¹ (метод сжатия compress), ZSTD ¹	Выполняется декомпрессия и проверка сжатых файлов
Образы дисков	ISO ¹	Извлекаются и проверяются дочерние файлы
Закодированные файлы	uuencoding ¹ (.uue, .uu)	Выполняется декодирование и проверка закодированных файлов
Файлы дампов памяти	minidump (.dmp)	Проверяются дочерние файлы (не отображаются в карточке задания)
Исполняемые файлы		
Установочные и пакетные файлы	APK, DEB, EGG, MSI, pyinstaller, RPM, WHEEL (.whl)	Проверяются дочерние файлы (не отображаются в карточке задания)
Контейнеры	CAB ¹ , CFB	Проверяются дочерние файлы (не отображаются в карточке задания)
Пакеты Java	JAR	Проверяется дочерние файлы (не отображаются в карточке задания)
Упаковщики	UPX	Проверяется дочерние файлы (не отображаются в карточке задания)
HTML-файлы	HTML	Извлекаются и проверяются ссылки

¹ При извлечении дочерних файлов установлено ограничение на размер файла в 512 МБ. Если файл превышает этот размер, то выполняется декодирование и проверка только фрагмента файла размером 512 МБ.

Тип	Формат	Примечание
Файлы офисных приложений		
Письма	EML, MSG, TNEF	Извлекаются почтовые заголовки, тело письма и вложенные файлы. Из файлов EML, MSG извлекаются и проверяются ссылки
Документы	DOC, MSOOXML (.docx, .docm, .dotx, .dotm), ODF (.odt), RTF	Проверяются дочерние файлы (не отображаются в карточке задания). Из файлов RTF извлекаются и проверяются ссылки. Из файлов MSOOXML и ODT извлекаются и проверяются ссылки, выделенные тегами
Таблицы	MSOOXML (.xlsx, .xlsm, .xltx, .xltm), ODF (.ods), XLS	Проверяются дочерние файлы (не отображаются в карточке задания). Из файлов MSOOXML и ODS извлекаются и проверяются ссылки, выделенные тегами
Презентации	MSOOXML (.pptx, .pptm, .potx, .potm, .ppsx, .ppsm), ODF (.odp), PPT	Проверяются дочерние файлы (не отображаются в карточке задания). Из файлов MSOOXML и ODP извлекаются и проверяются ссылки, выделенные тегами
Электронные книги	PDF	Проверяются дочерние файлы (не отображаются в карточке задания). Извлекаются и проверяются ссылки, выделенные тегами, а также ссылки, закодированные в QR-кодах на изображениях
Данные офисных приложений	OneNote (.one), PST	Извлекаются и проверяются дочерние файлы
Файлы других приложений		
Мультимедиа	SWF	Проверяются дочерние файлы (не отображаются в карточке задания)

9.2. Проверка объектов через веб-интерфейс

Через веб-интерфейс PT Email Security вы можете проверять файлы и ссылки. Поддерживается проверка файлов размером менее 1 ГБ. Если размер файла по ссылке превышает этот размер, скачивается и проверяется только часть файла в 1 ГБ. Для каждого файла и ссылки создается отдельное задание на проверку.

► Чтобы проверить объекты через интерфейс PT Email Security:

1. В главном меню нажмите кнопку **Проверить объекты**.
2. Если необходимо проверить файлы, нажмите кнопку **Файлы** и перетащите файлы в область загрузки.

Примечание. Вы можете изменить название файла, нажав в строке файла .

3. Если необходимо проверить ссылки, нажмите кнопку **Ссылки** и введите ссылки.
4. Настройте [параметры проверки объектов \(см. раздел 9.4\)](#).
5. Нажмите кнопку **Проверить**.

9.3. Поведенческий анализ в интерактивном режиме

► Чтобы выполнить поведенческий анализ файла в интерактивном режиме:

1. В главном меню нажмите кнопку **Проверить объекты**.
 2. Перетащите файл в область загрузки.
- Примечание.** Вы можете изменить название файла, нажав в строке файла .
3. В блоке параметров **Поведенческий анализ** выберите **Интерактивный режим**.
 4. Выберите образ виртуальной машины.
 5. Если требуется, настройте [параметры проверки \(см. раздел 9.4\)](#).
 6. Нажмите кнопку **Проверить**.

Откроется карточка задания. Начнется подготовка виртуальной машины.

7. Нажмите кнопку **Открыть консоль**.

Откроется VNC-консоль с операционной системой.

8. Выполните необходимые действия с файлом.

Примечание. Загруженный файл находится на рабочем столе операционной системы.

9. Нажмите кнопку **Завершить анализ**.

Откроется карточка задания. Начнется подготовка результатов поведенческого анализа.

9.4. Параметры проверки объектов

При проверке объектов через интерфейс вы можете настроить параметры проверки.

Поведенческий анализ (запускается автоматически)

При включении параметра вы сможете настроить поведенческий анализ файлов. Такой анализ выполняется только для [некоторых типов файлов \(см. приложение А\)](#). В ходе поведенческого анализа файл помещается в изолированную операционную систему, развернутую в виртуальной машине из указанного вами образа ВМ. Также вы можете выбрать способ проведения поведенческого анализа:

- **Запускается автоматически** — PT Email Security запускает файл в изолированной операционной системе и имитирует взаимодействие пользователя с этим файлом.
- **Запускается командой** — PT Email Security также запускает файл в изолированной операционной системе, но для запуска использует указанную вами команду.
- **Интерактивный режим** — через VNC-консоль вам предоставляется доступ в изолированную операционную систему, где вы можете выполнять любые действия с файлом и выявлять аномалии в его поведении.

Во всех случаях для выявления угроз PT Email Security анализирует действия файла при его запуске или открытии, включая сетевую активность, изменения системных настроек и реестра, запуск процессов, а также создание, изменение и удаление файлов.

Доступны следующие параметры поведенческого анализа файлов, запускаемого автоматически:

- **Режим с перезагрузкой ОС** — при включении этого режима PT Email Security отслеживает поведение файла в ОС до ее перезагрузки и после. Это помогает выявить вредоносное ПО, которое добавляет себя в автозагрузку и активируется только при запуске ОС.

Примечание. Режим с перезагрузкой ОС работает только в базовых образах ВМ Windows 7 SP1 x64, Windows 10 (1803) x64, Windows 10 (1803) x64 UEFI и Windows 11 (23H2) x64.

- **Образ виртуальной машины** — блок для выбора образов ВМ. Вы можете отметить флажками несколько образов ВМ. Выбирайте образы только с теми ОС, которые используются в вашей организации.
- **Типы проверяемых файлов** — раскрывающийся список для выбора типов и форматов проверяемых файлов (список доступен после выбора образов ВМ). Если типы загруженных на проверку файлов отличаются от тех, что указаны для образов, то такие файлы не будут проверяться методом поведенческого анализа.
- **Продолжительность наблюдения за файлом** — поля для ввода максимального времени поведенческого анализа в минутах и секундах. Время анализа не должно превышать 10 минут. При проверке архивов это время анализа каждого файла из архива. При выборе значения необходимо учитывать объем и скорость потока файлов в сочетании с производительностью аппаратных ресурсов.

Примечание. Для расчета продолжительности наблюдения за файлом вы можете использовать следующие рекомендации: если файлы приложений проверяются N минут, то презентации, таблицы и документы будут проверяться $1 + N/2$ минут, а файлы PDF — $0,5 + N/3$ минут. Например, если для файлов приложений вы указали продолжительность наблюдения 4 минуты, то для презентаций, таблиц и документов рекомендуется указать 3 минуты, а для файлов PDF — примерно 2 минуты.

- **Расшифровывать и анализировать HTTPS-трафик** — при установленном флажке для расшифровки защищенного HTTPS-трафика между проверяемым файлом и внешними узлами используется собственный сертификат PT Email Security. Если необходимо выявить вредоносное ПО, которое проверяет подлинность сертификатов и прекращает свою активность при обнаружении подмены, вы можете снять флажок.
- **Отключить запись видео** — установка флажка позволяет отключить запись видео поведения файлов в ОС. При снятии флажка видео записывается, но при этом увеличивается нагрузка на систему.
- **Использовать результаты предыдущих проверок** — при установленном флажке используются результаты предыдущих проверок файлов методом поведенческого анализа. Результат анализа каждого файла хранится в оперативной памяти сервера PT Email Security в течение 48 часов. Если в течение этого времени такой же файл повторно поступает на поведенческий анализ в том же образе ВМ с такими же настройками, повторный анализ файла не проводится, в этом случае используется результат предыдущей проверки. При снятии флажка результаты предыдущих проверок не используются, но при этом увеличивается нагрузка на систему.

Поведенческий анализ (запускается командой)

Доступны следующие параметры поведенческого анализа файлов, запускаемого командой:

- **Запускаемый файл** — раскрывающийся список для выбора файла, который будет запущен указанной ниже командой.
- **Команда для запуска файла** — поле для ввода команды, которую PT Email Security будет использовать для запуска файла при поведенческом анализе. Если вы хотите запустить файл стандартной командой PT Email Security, используйте переменную `{default_cmd}`, например, добавив к ней дополнительные параметры. Для указания пути к запускаемому файлу используйте переменную `{file}`, а для указания пути к другим проверяемым файлам — переменные `{extra1}`, `{extra2}` и так далее. Примеры команд:
 - В образах Windows: для запуска файла с расширением `.exe` вы можете ввести команду `{file}`; для запуска файла `.ps1` — команду `powershell -NonInteractive -File {file}`.
 - В образе Astra Linux: для запуска файла с расширением `.sh` вы можете ввести команду `/usr/bin/fly-term -noclose -e /bin/bash {file}`; для запуска файла `.elf` — команду `/usr/bin/fly-term -noclose -e {file}`.

- **Режим с перезагрузкой ОС** — при включении этого режима PT Email Security отслеживает поведение файла в ОС до ее перезагрузки и после. Это помогает выявить вредоносное ПО, которое добавляет себя в автозагрузку и активируется только при запуске ОС.

Примечание. Режим с перезагрузкой ОС работает только в базовых образах BM Windows 7 SP1 x64, Windows 10 (1803) x64, Windows 10 (1803) x64 UEFI и Windows 11 (23H2) x64.

- **Образ виртуальной машины** — блок для выбора образов BM. Вы можете отметить флажками несколько образов BM. Выбирайте образы только с теми ОС, которые используются в вашей организации.
- **Продолжительность наблюдения за файлом** — поля для ввода максимального времени поведенческого анализа в минутах и секундах. Время анализа не должно превышать 10 минут. При проверке архивов это время анализа каждого файла из архива. При выборе значения необходимо учитывать объем и скорость потока файлов в сочетании с производительностью аппаратных ресурсов.

Примечание. Для расчета продолжительности наблюдения за файлом вы можете использовать следующие рекомендации: если файлы приложений проверяются N минут, то презентации, таблицы и документы будут проверяться $1 + N/2$ минут, а файлы PDF — $0,5 + N/3$ минут. Например, если для файлов приложений вы указали продолжительность наблюдения 4 минуты, то для презентаций, таблиц и документов рекомендуется указать 3 минуты, а для файлов PDF — примерно 2 минуты.

- **Расшифровывать и анализировать HTTPS-трафик** — при установленном флажке для расшифровки защищенного HTTPS-трафика между проверяемым файлом и внешними узлами используется собственный сертификат PT Email Security. Если необходимо выявить вредоносное ПО, которое проверяет подлинность сертификатов и прекращает свою активность при обнаружении подмены, вы можете снять флажок.
- **Отключить запись видео** — установка флажка позволяет отключить запись видео поведения файлов в ОС. При снятии флажка видео записывается, но при этом увеличивается нагрузка на систему.

Поведенческий анализ (интерактивный режим)

Доступны следующие параметры интерактивного режима поведенческого анализа файлов:

- **Образ виртуальной машины** — переключатель для выбора образа BM.
- **Продолжительность наблюдения за файлом** — поля для ввода максимального времени поведенческого анализа в минутах и секундах. Время анализа не должно превышать 30 минут.

- **Расшифровывать и анализировать HTTPS-трафик** — при установленном флажке для расшифровки защищенного HTTPS-трафика между проверяемым файлом и внешними узлами используется собственный сертификат PT Email Security. Если необходимо выявить вредоносное ПО, которое проверяет подлинность сертификатов и прекращает свою активность при обнаружении подмены, вы можете снять флажок.
- **Отключить запись видео** — установка флажка позволяет отключить запись видео поведения файлов в ОС. При снятии флажка видео записывается, но при этом увеличивается нагрузка на систему.

Анализ файлов, найденных в черном или белом списке

В PT Email Security предусмотрена возможность добавления файлов в черный или белый список. По умолчанию такие файлы не проверяются, файлы из черного списка всегда считаются опасными, из белого списка — безопасными.

Продолжать проверку файла после его обнаружения в одном из списков — флажок для включения проверки файлов, которые уже добавлены в исключения.

Проверка архивов

В этом блоке вы можете настроить параметры проверки архивов. Доступны следующие параметры:

- **Пароли для архивов** — поле для ввода паролей, которые будут использоваться при распаковке архивов помимо стандартных. Необходимо вводить по одному паролю в каждой строке.

Примечание. Список стандартных паролей указан на странице **Основные параметры** в разделе **Система**.

- **Глубина распаковки архивов** — поле для ввода максимального количества вложенных друг в друга архивов, которые будут распаковываться при проверке. Если распаковывать архивы не требуется, вы можете ввести 0, тогда архивы будут проверяться как обычные файлы. Увеличение глубины распаковки архивов снижает скорость проверки.
- **Определять как потенциально опасные** — в этом блоке параметров вы можете указать признаки архивов, по которым PT Email Security будет относить их к потенциально опасным:
 - **Зашифрованные и нераспакованные архивы** — защищенные паролем архивы, для которых не удалось подобрать пароль.
 - **Архивы с превышенной глубиной распаковки** — архивы, содержащие вложенные архивы, количество которых превышает значение, указанное в параметре **Глубина распаковки архивов**.

Проверка контента по ссылкам

Проверка контента выполняется по добавленным ссылкам и по ссылкам, извлеченным из добавленных файлов. По ссылкам, которые не содержат индикаторов компрометации, скачивается контент и в виде файлов отправляется на проверку. Для извлеченных из файлов ссылок вы можете настроить дополнительные параметры фильтрации:

- **Доменные имена, IP-адреса узлов и подсетей для проверки контента** — поле для ввода проверяемых адресов. Контент будет скачиваться и проверяться только по ссылкам на указанные адреса. Эвристический анализ таких ссылок не выполняется. Вы можете указать имена доменов, поддоменов, IP-адреса узлов или адреса подсетей в формате CIDR. Ссылки на IP-адрес и доменное имя одного и того же ресурса считаются разными ссылками. При вводе адресов вы можете использовать звездочку:
 - Если необходимо проверять контент по ссылкам на любые адреса, вы можете ввести *.

Внимание! При пустом поле контент будет проверяться только по тем ссылкам, которые система определит как подозрительные.

 - Если необходимо проверять контент по ссылкам на определенный домен, вы можете ввести *<Имя домена>, например *example.com.
 - Если необходимо проверять контент по ссылкам на любые поддомены одного домена, вы можете ввести *.<Имя домена>, например *.example.com.
- **Исключаемые доменные имена, IP-адреса узлов и подсетей** — поле для ввода исключаемых адресов. По ссылкам на эти адреса контент скачиваться не будет. Вы можете указать имена доменов, поддоменов, IP-адреса узлов или адреса подсетей в формате CIDR. При вводе адресов вы можете использовать звездочку. Приоритет исключаемых адресов выше приоритета адресов для проверки.
- **Исключаемые категории ссылок** — раскрывающийся список для выбора исключаемых из проверки категорий ссылок. По ссылкам, отнесенным к этим категориям, контент проверяться не будет. Если ссылке присвоена какая-то дополнительная категория, кроме выбранных, контент по ссылке будет проверен. Список категорий ссылок совпадает с перечнем устанавливаемых для ссылок [меток \(см. приложение Г\)](#).
- **Включить эвристику** — при установленном флажке контент будет проверяться по ссылкам, которые система определит как подозрительные.
- **Ограничить количество ссылок для скачивания до** — при установленном флажке вы можете указать количество ссылок в задании, по которым будет скачиваться и проверяться контент. При снятом флажке контент будет проверяться по всем извлеченным в задании ссылкам.

Категории опасных и потенциально опасных ссылок

При проверке ссылок PT Email Security выполняет категоризацию ссылок и устанавливает для них соответствующие [метки](#) (см. приложение Г). В этом блоке параметров вы можете настроить правило, по которому PT Email Security будет относить ссылки к опасным или потенциально опасным объектам в зависимости от их категорий. Доступны следующие параметры:

- **Назначаемый уровень опасности** — переключатель для выбора назначаемого ссылкам уровня опасности: **Опасный** или **Потенциально опасный**.
- **Считать опасными (потенциально опасными)** — переключатель для выбора способа определения содержащих угрозу ссылок:
 - **Только ссылки указанных категорий** — к ссылкам с угрозами будут отнесены ссылки указанных ниже категорий.
 - **Все ссылки, кроме ссылок указанных категорий** — к ссылкам с угрозами будут отнесены ссылки, не относящиеся ни к одной из указанных категорий.
- **Категории ссылок** — раскрывающийся список для выбора категорий ссылок.

Дополнительные признаки опасных и потенциально опасных файлов

При проверке файлов PT Email Security выявляет различные свойства файлов и по ряду признаков устанавливает для них [метки](#) (см. приложение Г). В этом блоке параметров вы можете настроить дополнительное правило, по которому PT Email Security будет относить файлы к опасным или потенциально опасным объектам в зависимости от их свойств. Доступны следующие параметры:

- **Назначаемый уровень опасности** — переключатель для выбора назначаемого файлу уровня опасности: **Опасный** или **Потенциально опасный**.
- **Считать опасными (потенциально опасными)** — переключатель для выбора способа определения содержащих угрозу файлов:
 - **Только файлы со всеми указанными признаками** — к файлам с угрозами будут отнесены файлы, которые соответствуют всем указанным ниже признакам.
 - **Все файлы, кроме файлов с указанными признаками** — к файлам с угрозами будут отнесены файлы, которые не соответствуют хотя бы одному из указанных признаков.
- **Типы файлов** — раскрывающийся список для выбора типов и форматов файлов.

Примечание. Если в поле **Типы файлов** указано несколько значений, файл будет отнесен к файлам с угрозами, если относится к одному из указанных типов или форматов (по логическому правилу ИЛИ). То же самое относится к полям **Маски имен файлов**, **Маски MIME-типов**, **Метки**.

- **Маски имен файлов** — поле для ввода имен и масок имен файлов.

- **Маски MIME-типов** — поле для ввода MIME-типов и масок MIME-типов файлов, например `application/xml, text/*`.
- **Метки** — раскрывающийся список для выбора меток файлов (список недоступен для варианта **Все файлы, кроме файлов с указанными признаками**).

Использовать тестовые YARA-правила

Если включено средство проверки по пользовательским YARA-правилам, для проверки объектов используются действующие YARA-правила. Дополнительно для отладки новых YARA-правил вы можете включить проверку объектов по тестовым YARA-правилам. Результат такой проверки отображается в карточке объекта, но не влияет на вердикт по объекту.

9.5. Управление очередью файлов на поведенческий анализ

Отправленные на поведенческий анализ файлы поступают на проверку в порядке очереди. Файлы в очереди сортируются по времени создания заданий на проверку, из которых они получены, и по важности источника файлов. Вы можете управлять очередью файлов, повышая и снижая приоритет проверки выбранных файлов в очереди или устанавливая для них нужный приоритет. Доступны следующие приоритеты проверки файлов в порядке возрастания: «Минимальный», «Низкий», «Средний», «Высокий», «Срочный». Для снижения нагрузки на PT Email Security вы можете отменить поведенческий анализ выбранных файлов или полностью очистить очередь. При этом проверка таких файлов другими средствами проверки будет продолжена.

Для управления очередью файлов, отправленных на поведенческий анализ, предназначена страница **Средства проверки → Поведенческий анализ → Очередь файлов на анализ**.

⬆ В начало очереди ⬆ В конец очереди ⬆ Изменить приоритет ⬆ Повысить приоритет ⬇ Снизить приоритет ⌛ Отменить ПА 🗑 Очистить очередь ⚙ ↺									
☒	Очередь	Имя файла	Формат файла	Приоритет	Добавлен За последние 7 д...	Статус ПА 2 значения	До завершения ПА	Метки	Название образа VM
☐		1275.pdf	PDF	—	Сегодня, 14:23	Выполняется Сегодня, 14:23	Меньше минуты		win10-1803-x64
☐		psexec	BAT	—	Сегодня, 14:30	Выполняется Сегодня, 14:30	Меньше минуты		win10-1803-x64
☐		web-shells	BAT	—	Сегодня, 14:30	Выполняется Сегодня, 14:33	Меньше минуты		win10-1803-x64
☐		Rundll32.bat	BAT	—	Сегодня, 14:30	Выполняется Сегодня, 14:38	Меньше минуты		win10-1803-x64
☐	1	MSTHA.bat	BAT	Средний	Сегодня, 14:30	Запланирован Сегодня, 14:30	Меньше минуты		win10-1803-x64
☐	2	powerdump.bat	BAT	Средний	Сегодня, 14:30	Запланирован Сегодня, 14:30	Меньше минуты		win10-1803-x64
☒	3	userinit-mp...script	BAT	Средний	Сегодня, 14:30	Запланирован Сегодня, 14:30	Меньше минуты	⬆ ⬆ ⬆ ⬆ ⌛	
☐	4	WML.bat	BAT	Средний	Сегодня, 14:30	Запланирован Сегодня, 14:30	Меньше минуты		win10-1803-x64
Всего 29									1 < >

Рисунок 5. Страница **Очередь файлов на поведенческий анализ**

В панели инструментов страницы расположены:

- Кнопка **В начало очереди** для повышения приоритета выбранных файлов в очереди до максимального.
- Кнопка **В конец очереди** для снижения приоритета выбранных файлов в очереди до минимального.
- Кнопка **Изменить приоритет** с раскрывающимся списком для выбора приоритета выбранных файлов: **Срочный, Высокий, Средний, Низкий, Минимальный**.
- Кнопка **Повысить приоритет** для повышения приоритета выбранных файлов в очереди на один уровень.
- Кнопка **Снизить приоритет** для снижения приоритета выбранных файлов в очереди на один уровень.
- Кнопка **Отменить ПА** для отмены поведенческого анализа выбранных файлов.
- Кнопка **Очистить очередь** для отмены поведенческого анализа всех файлов в очереди, для которых он еще не был запущен.
- Кнопка  для выбора столбцов, которые должны отображаться в таблице.
- Кнопка  для обновления данных в таблице.

В рабочей области страницы расположена таблица со списком файлов, отправленных на поведенческий анализ. По умолчанию файлы в таблице расположены согласно их приоритету в очереди на поведенческий анализ.

Примечание. Нажимая на заголовки столбцов таблицы, вы можете настроить фильтрацию файлов в таблице или выполнить поиск файлов. Используя стрелки в заголовках столбцов, вы можете настроить сортировку файлов.

В зависимости от вашего выбора, таблица может содержать следующие столбцы с информацией о файлах:

- **Очередь** — в столбце указан порядковый номер файла в очереди на поведенческий анализ или значок , если для файла поведенческий анализ уже выполняется.
- **Имя файла** — в столбце указано имя файла.
- **Формат файла** — в столбце указан формат файла.
- **Приоритет** — в столбце указан приоритет файла в очереди.
- **Добавлен** — в столбце указаны дата и время добавления файла в очередь.

- **Статус ПА** — в столбце указаны статус поведенческого анализа файла, дата и время последней смены статуса:
 - **Запланирован** — поведенческий анализ будет запущен согласно приоритету файла в очереди.
 - **Запускается** — выполняется подготовка виртуальной среды для запуска поведенческого анализа.
 - **Выполняется** — поведенческий анализ выполняется.
 - **Ожидается завершение для дубликата** — уже выполняется поведенческий анализ такого же файла с теми же параметрами проверки. Результат его анализа будет использован для обоих файлов.
 - **Обработка результатов** — сохраняется результат поведенческого анализа.
 - **Завершен по тайм-ауту** — поведенческий анализ завершен, поскольку превышено указанное в параметрах проверки время наблюдения за файлом.
 - **Выполнен** — поведенческий анализ выполнен.
 - **Выполнен с ошибкой** — поведенческий анализ файла выполнен с ошибкой.
- **До завершения ПА** — в столбце указано время до завершения поведенческого анализа.
- **MIME-тип** — в столбце указан MIME-тип файла.
- **Метки** — в столбце указаны метки файла.
- **Название образа ВМ** — в столбце указано название образа ВМ, выбранного для поведенческого анализа файла.
- **Команда для запуска** — в столбце указана команда для запуска файла при поведенческом анализе.
- **Задание** — в столбце указано название задания, в котором файл поступил на проверку.
- **Источник** — в столбце указан источник, от которого файл поступил на проверку:
 -  **Веб-интерфейс** — имя пользователя, который отправил файл на проверку через веб-интерфейс PT Email Security, и логин его учетной записи.
 -  **Хранилище (повторная проверка)** — хранилище объектов при повторной проверке файла из хранилища.
 -  — почтовый сервер или служба Checkme.
 -  — ICAP-сервер или PT NAD.
 -  — общая папка или папка-шлюз.
 - API** — стороннее приложение через API.

Изменение приоритета файлов в очереди

- ▶ Чтобы изменить приоритет файлов в очереди на поведенческий анализ:
 1. В главном меню выберите **Средства проверки** → **Поведенческий анализ** → **Очередь файлов на анализ**.
 2. В столбце **Очередь** отметьте файлы.
 3. В панели инструментов нажмите кнопку **Изменить приоритет** → **<Приоритет>**.

Повышение приоритета файлов в очереди

- ▶ Чтобы повысить приоритет файлов в очереди на поведенческий анализ:
 1. В главном меню выберите **Средства проверки** → **Поведенческий анализ** → **Очередь файлов на анализ**.
 2. В столбце **Очередь** отметьте файлы.
 3. Если требуется повысить приоритет на один уровень, в панели инструментов нажмите кнопку **Повысить приоритет**.
 4. Если требуется повысить приоритет до максимального уровня, в панели инструментов нажмите кнопку **В начало очереди**.

Снижение приоритета файлов в очереди

- ▶ Чтобы снизить приоритет файлов в очереди на поведенческий анализ:
 1. В главном меню выберите **Средства проверки** → **Поведенческий анализ** → **Очередь файлов на анализ**.
 2. В столбце **Очередь** отметьте файлы.
 3. Если требуется снизить приоритет на один уровень, в панели инструментов нажмите кнопку **Снизить приоритет**.
 4. Если требуется снизить приоритет до минимального уровня, в панели инструментов нажмите кнопку **В конец очереди**.

Отмена поведенческого анализа файлов

- ▶ Чтобы отменить поведенческий анализ файлов:
 1. В главном меню выберите **Средства проверки** → **Поведенческий анализ** → **Очередь файлов на анализ**.
 2. В столбце **Очередь** отметьте файлы.
 3. В панели инструментов нажмите кнопку **Отменить ПА**.

Очистка очереди файлов на поведенческий анализ

► Чтобы очистить очередь файлов на поведенческий анализ:

1. В главном меню выберите **Средства проверки** → **Поведенческий анализ** → **Очередь файлов на анализ**.
2. В панели инструментов нажмите кнопку **Очистить очередь**.

В течение нескольких минут будет выполнен поведенческий анализ тех файлов из очереди, для которых он уже запущен, для остальных файлов в очереди он будет отменен.

В панели инструментов страницы расположены:

- Кнопка **<Название фильтра>** для выбора фильтра. По кнопке раскрывается меню, в котором вы можете выбрать один из сохраненных фильтров или фильтр по умолчанию. В верхней части меню доступно поле для быстрого поиска фильтра.
- Кнопка  для выбора дополнительных действий с фильтром. После настройки параметров фильтрации по этой кнопке вы можете сохранить их как новый фильтр или сбросить все изменения. После изменения параметров созданного ранее фильтра по этой кнопке вы можете сохранить для него измененные параметры фильтрации, сохранить параметры фильтрации как новый фильтр, сбросить все изменения, переименовать фильтр или удалить его.
- Кнопка  для выбора фильтра по умолчанию.
- Переключатель **Режим QL-запросов** для создания фильтра с помощью языка запросов QL. В этом режиме появляется поле для ввода QL-запросов, кнопки  и  для выбора предыдущего или следующего запроса и кнопка  для просмотра списка выполненных ранее запросов.
- Кнопка  для выбора столбцов, которые должны отображаться в таблице.
- Кнопка  для обновления данных в таблице.
- Кнопка  для настройки автоматического обновления данных в таблице.
- Кнопка **Скачать отчет** для сохранения списка заданий в файле формата CSV.

В рабочей области страницы расположена таблица со списком заданий на проверку. По ссылке в строке задания вы можете открыть карточку задания. В зависимости от вашего выбора, таблица может содержать следующие столбцы с информацией о задании:

- **Статус проверки** — в столбце отображается значок статуса проверки задания:
 -  — проверка не выполнена;
 -  — проверка выполнена частично;
 -  — проверка завершена;
 -  — выполняется проверка.
- **Решение о блокировке** — в столбце отображается значок, указывающий на решение о допуске объекта задания в информационную систему организации:
 -  — заблокировать;
 -  — пропустить;
 -  — не требуется.
- **Карантин** — в столбце отображается значок, показывающий, был ли файл помещен в карантин:

 — в карантине;

 — удалено из карантина;

Отсутствие значка указывает на то, что файл не помещался в карантин.

- **Дата создания** — в столбце указаны дата и время добавления задания. По умолчанию в таблице отображаются задания за последние 7 дней.
- **Задание** — в столбце указано название проверяемого объекта.
- **Источник** — в столбце указан источник, от которого объект поступил на проверку:

 **Веб-интерфейс** — имя пользователя, который отправил объект на проверку через веб-интерфейс PT Email Security, и логин его учетной записи.

 **Хранилище (повторная проверка)** — хранилище объектов при повторной проверке объектов из хранилища.

 — почтовый сервер или служба Checkme.

 — ICAP-сервер или PT NAD.

 — общая папка или папка-шлюз.

API — стороннее приложение через API.

- **Вердикт** — в столбце указан вердикт по заданию и, если обнаружены объекты с вредоносным ПО, тип обнаруженного ПО.
- **Поведенческий анализ** — в столбце отображается значок, показывающий результат поведенческого анализа:

 — обнаружены опасные файлы;

 — обнаружены потенциально опасные файлы;

 — поведенческий анализ выполнен частично или с ошибками;

 — угроз не обнаружено;

Отсутствие значка указывает на то, что поведенческий анализ не проводился.

- **Откуда > Куда** — в столбце указана информация об отправителе объекта:
 - Если объект отправлен через веб-интерфейс PT Email Security, в столбце указан логин учетной записи пользователя.
 - Если объект поступил на проверку через службу Checkme, — адрес электронной почты, с которого пришло письмо.
 - Если объект поступил с почтового сервера, — адреса электронной почты отправителя и получателя письма.

Для других источников информация в столбце не указывается.

- **Время до решения о блокировке** — в столбце отображается время от создания задания до принятия решения о блокировке в секундах.
- **Время до вердикта** — в столбце отображается время от создания задания до вынесения вердикта в секундах.

Настройка столбцов таблицы

- ▶ Чтобы настроить столбцы в таблице заданий:

1. В главном меню выберите **Задания**.
2. Нажмите .
3. Выберите столбцы.

Примечание. Вы можете выбрать набор столбцов по умолчанию, нажав кнопку **Сбросить**.

Выбранные столбцы появятся в таблице.

Настройка фильтра по заданиям

Фильтровать задания в таблице можно по любым столбцам.

- ▶ Чтобы настроить фильтр заданий:

1. В главном меню выберите **Задания**.
2. Настройте столбцы таблицы, по которым нужно отфильтровать задания.
3. Если требуется фильтровать задания по статусу проверки:
 - Нажмите на заголовок столбца **Статус проверки**.
 - Выберите статусы.
4. Если требуется фильтровать задания по времени создания:
 - Нажмите на заголовок столбца **Дата создания**.
 - Выберите предустановленный период или настройте свой.
 - Нажмите кнопку **Применить**.
5. Если требуется фильтровать задания по названию поступившего на проверку объекта:
 - Нажмите на заголовок столбца **Задание**.
 - Введите часть названия или название объекта целиком.

Примечание. Вы можете использовать маски с подстановочными знаками * и ?.

6. Если требуется фильтровать задания по источникам объектов:

- Нажмите на заголовок столбца **Источник**.
 - Выберите источники.
7. Если требуется фильтровать задания по вердикту:
 - Нажмите на заголовок столбца **Вердикт**.
 - Выберите типы вредоносного ПО.
 8. Если требуется фильтровать задания по уровню опасности обнаруженного вредоносного ПО:
 - Нажмите на заголовок столбца **Уровень опасности**.
 - Выберите уровни опасности.
 9. Если требуется фильтровать задания по результатам поведенческого анализа:
 - Нажмите на заголовок столбца **Поведенческий анализ**.
 - Выберите результаты поведенческого анализа.
 10. Если требуется фильтровать задания по другим столбцам, настройте фильтрацию аналогичным образом.

Фильтр заданий настроен, в таблице отображаются задания, которые удовлетворяют всем указанным параметрам.

Поиск заданий с помощью языка запросов QL

► Чтобы найти задания с помощью QL-запроса:

1. В главном меню выберите **Задания**.
2. Включите режим ввода QL-запросов.
3. Введите запрос, используя [синтаксис языка запросов QL \(см. приложение Д\)](#).

Например:

```
age < 30d AND (task.correlated.state != UNKNOWN AND
task.correlated.verdict.threat.classification IN ("TROJAN")) AND
task.sandbox.correlated.verdict.threat.level = DANGEROUS
```

4. Нажмите клавишу Enter.

В таблице появятся задания, которые удовлетворяют QL-запросу.

Сохранение фильтра по заданиям

Сохраненные вами фильтры не видны другим пользователям PT Email Security.

- ▶ Чтобы сохранить фильтр заданий:
 1. В главном меню выберите **Задания**.
 2. Настройте фильтр по заданиям.
 3. В панели инструментов нажмите  → **Сохранить как новый**.
 4. Введите название фильтра и нажмите кнопку **Создать**.

Фильтр заданий сохранен.

Сохранение отчета по заданиям

Вы можете сохранить отчет по заданиям в формате CSV. Отчет будет содержать информацию по отфильтрованным заданиям.

- ▶ Чтобы сохранить отчет по заданиям:
 1. В главном меню выберите **Задания**.
 2. Настройте фильтр по заданиям.
 3. Нажмите кнопку **Скачать отчет**.

Файл отчета с названием `tasks-<Дата и время скачивания>Z.csv` сохранен на ваш компьютер.

10.2. Поиск по объектам

Все объекты, поступающие на проверку в PT Email Security, в виде файлов сохраняются в хранилище. Также в хранилище сохраняются все дочерние объекты, полученные при проверке. Для каждого объекта создается карточка объекта. Для поиска по объектам предназначена страница **Объекты**. Страница открывается при выборе в главном меню раздела **Объекты**.

По умолчанию										Режим QL-запросов		⚙️ 🔍 ⋮		📄 Скачать отчет	
С...	Дата создания ... За последние 7 дн...	↓	Объект	Тип объекта	Тип элемента в струк...	Источник	⬆	Вердикт	Уровень...	⬆	Откуда > Куда	Поведенческий анализ			
✓	29 окт, 10:57		script.xsl	Файл	Карточка объекта	👤 Ivan (Ivanov)		Угроз не обнаружено			Ivanov				
✓	29 окт, 10:57		① 36d5946f07cdfd	Дамп памяти...	Карточка объекта	👤 Ivan (Ivanov)		Потенциально н...	① ⚡ ⚡ ⚡		Ivanov				
✓	29 окт, 10:57		① 190f09c57f01aa	Дамп памяти...	Карточка объекта	👤 Ivan (Ivanov)		Угроз не обнаружено			Ivanov				
✓	29 окт, 10:57		users/brenda/appd	Dropped файл	Карточка объекта	👤 Ivan (Ivanov)		Угроз не обнаружено			Ivanov				
✓	29 окт, 10:57		users/brenda/appd	Dropped файл	Карточка объекта	👤 Ivan (Ivanov)		Угроз не обнаружено			Ivanov				
✓	29 окт, 10:57		procdump64.exe	Файл	Карточка поведенчес...	👤 Ivan (Ivanov)		Пентест-инстру...	① ⚡ ⚡ ⚡		Ivanov	🚩 Обнаружены поте...			
✓	29 окт, 10:57		procdump64.exe	Файл	Карточка объекта	👤 Ivan (Ivanov)		Пентест-инстру...	① ⚡ ⚡ ⚡		Ivanov				
✓	29 окт, 10:57		① f67a5b2dfedc13	Дамп памяти...	Карточка объекта	👤 Ivan (Ivanov)		Угроз не обнаружено			Ivanov				
✓	29 окт, 10:57		① 14dfa71ba6867e	Дамп памяти...	Карточка объекта	👤 Ivan (Ivanov)		Угроз не обнаружено			Ivanov				
✓	29 окт, 10:57		users/brenda/appd	Dropped файл	Карточка объекта	👤 Ivan (Ivanov)		Угроз не обнаружено			Ivanov				
Всего 321															
1 2 3 4 5 ... 7 < >															

Рисунок 7. Страница **Объекты**

В панели инструментов страницы расположены:

- Кнопка **<Название фильтра>** для выбора фильтра. По кнопке раскрывается меню, в котором вы можете выбрать один из сохраненных фильтров или фильтр по умолчанию. В верхней части меню доступно поле для быстрого поиска фильтра.
- Кнопка  для выбора дополнительных действий с фильтром. После настройки параметров фильтрации по этой кнопке вы можете сохранить их как новый фильтр или сбросить все изменения. После изменения параметров созданного ранее фильтра по этой кнопке вы можете сохранить для него измененные параметры фильтрации, сохранить параметры фильтрации как новый фильтр, сбросить все изменения, переименовать фильтр или удалить его.
- Кнопка  для выбора фильтра по умолчанию.
- Переключатель **Режим QL-запросов** для создания фильтра с помощью языка запросов QL. В этом режиме появляется поле для ввода QL-запросов, кнопки  и  для выбора предыдущего или следующего запроса и кнопка  для просмотра списка выполненных ранее запросов.
- Кнопка  для выбора столбцов, которые должны отображаться в таблице.
- Кнопка  для обновления данных в таблице.
- Кнопка  для настройки автоматического обновления данных в таблице.
- Кнопка **Скачать отчет** для сохранения списка проверенных объектов в файле формата CSV.

В рабочей области страницы расположена таблица со списком проверенных объектов. По ссылке в строке объекта вы можете открыть карточку объекта. В зависимости от вашего выбора таблица может содержать следующие столбцы с информацией об объектах:

- **Статус проверки** — в столбце отображается значок статуса проверки объекта:
 -  — проверка не выполнена;
 -  — проверка выполнена частично;
 -  — проверка завершена;
 -  — выполняется проверка.
- **Дата создания задания** — в столбце указаны дата и время добавления задания на проверку объекта. По умолчанию в таблице отображаются объекты заданий, созданных за последние 7 дней.
- **Объект** — в столбце указано название объекта, с которым он впервые поступил на проверку.

- **Тип объекта** — в столбце указан тип объекта.
- **Тип элемента в структуре задания** — в столбце указано, является ли этот элемент карточкой объекта или карточкой поведенческого анализа.
- **Источник** — в столбце указан источник, от которого объект поступил на проверку:

 **Веб-интерфейс** — имя пользователя, который отправил объект на проверку через веб-интерфейс PT Email Security, и логин его учетной записи.

 **Хранилище (повторная проверка)** — хранилище объектов при повторной проверке объектов из хранилища.

 — почтовый сервер или служба Checkme.

 — ICAP-сервер или PT NAD.

 — общая папка или папка-шлюз.

API — стороннее приложение через API.

- **Вердикт** — в столбце указан вердикт по объекту. Если в объекте обнаружено вредоносное ПО, указан его тип. По кнопке  вы можете посмотреть, какими средствами проверки вредоносное ПО было обнаружено.
- **Откуда > Куда** — в столбце указана информация об отправителе объекта:
 - Если объект отправлен через веб-интерфейс PT Email Security, в столбце указан логин учетной записи пользователя.
 - Если объект поступил на проверку через службу Checkme, — адрес электронной почты, с которого пришло письмо.
 - Если объект поступил с почтового сервера, — адреса электронной почты отправителя и получателя письма.

Для других источников информация в столбце не указывается.

- **Поведенческий анализ** — в столбце отображается значок, показывающий результат поведенческого анализа:

 — обнаружены опасные файлы;

 — обнаружены потенциально опасные файлы;

 — поведенческий анализ выполнен частично или с ошибками;

 — угроз не обнаружено;

Отсутствие значка указывает на то, что поведенческий анализ не проводился.

- **Размер объекта** — в столбце указан размер объекта.
- **Идентификатор задания** — в столбце указан идентификатор задания, по которому проверен объект.

- **Объект получен** — в столбце указано, откуда получен объект:
 - **От источника** — объект поступил на проверку от источника.
 - **Из архива** — файл получен в результате распаковки архива.
 - **Из письма** — файл является телом или вложением письма.
 - **Из тела письма** — ссылка извлечена из тела письма.
 - **Из файла** — ссылка извлечена из файла, тела письма или вложения.
 - **По ссылке** — файл скачан по ссылке.
 - **Из HTTP-сообщения** — файл получен в результате HTTP-запроса.
 - **В результате ПА** — объект является артефактом поведенческого анализа.
- **Причина вердикта** — для объектов с угрозами в столбце указаны средства проверки, которыми эта угроза была обнаружена. Если указано **Наследуемый вердикт**, то причиной вердикта стал результат проверки дочерних объектов.
- **Формат файла** — в столбце указан формат файла.
- **MIME-тип** — в столбце указан формат файла, записанный в виде MIME-типа.
- **SHA-256, SHA-1, MD5, SSDEEP** — в столбцах указана хеш-сумма файла в различных форматах.
- **Метки** — в столбце указаны особенности объекта.
- **Черный и белый списки** — в столбце указано, находился ли файл в черном или белом списке на момент проверки:
 -  **В черном списке;**
 -  **В белом списке;**

Если ничего не указано, то файл на момент проверки отсутствовал в списках.
- **Название образа ВМ** — в столбце указано название образа ВМ, на котором выполнялся поведенческий анализ файла.
- **Продолжительность анализа** — в столбце указано время выполнения поведенческого анализа файла в минутах.
- **Поведенческий анализ (результат проверки)** — в столбце указан тип вредоносного ПО, обнаруженного при поведенческом анализе..
- **Поведенческий анализ (обнаруженное ВПО)** — в столбце указано название вредоносного ПО, обнаруженного при поведенческом анализе.
- **Потенциально опасное поведение** — в столбце указана информация о подозрительном поведении файла, обнаруженном при поведенческом анализе.

- **Анализ с перезагрузкой ОС** — в столбце указан режим поведенческого анализа файла.
- **Родительский процесс** — в столбце указано название родительского процесса, связанного с вредоносным ПО, которое было обнаружено при поведенческом анализе.
- **<Средство проверки> (результат проверки)** — в столбце указан тип вредоносного ПО, обнаруженного этим средством проверки.
- **<Средство проверки> (обнаруженное ВПО)** — в столбце указано название вредоносного ПО, обнаруженного этим средством проверки.

Примечание. Вы можете добавить столбцы для результатов проверки с помощью антивирусов, средства проверки PT ESC и по дополнительным критериям определения потенциально опасных файлов. Также вы можете добавить столбцы для обнаруженного этими средствами проверки ВПО.

Настройка столбцов таблицы

- ▶ Чтобы настроить столбцы в таблице объектов:

1. В главном меню выберите **Объекты**.
2. Нажмите .
3. Выберите столбцы.

Примечание. Вы можете выбрать набор столбцов по умолчанию, нажав кнопку **Сбросить**.

Выбранные столбцы появятся в таблице.

Настройка фильтра по объектам

Фильтровать объекты в таблице можно по любым столбцам.

- ▶ Чтобы настроить фильтр объектов:

1. В главном меню выберите **Объекты**.
2. Настройте столбцы таблицы, по которым нужно отфильтровать объекты.
3. Если требуется фильтровать объекты по дате создания задания:
 - Нажмите на заголовок столбца **Дата создания**.
 - Выберите предустановленный период или настройте свой.
 - Нажмите кнопку **Применить**.
4. Если требуется фильтровать объекты по названию:
 - Нажмите на заголовок столбца **Объект**.
 - Введите часть названия или название объекта целиком.

Примечание. Вы можете использовать маски с подстановочными знаками * и ?.

5. Если требуется фильтровать объекты по источникам:
 - Нажмите на заголовок столбца **Источник**.
 - Выберите источники.
6. Если требуется фильтровать объекты по вердикту:
 - Нажмите на заголовок столбца **Вердикт**.
 - Выберите типы вредоносного ПО.
7. Если требуется фильтровать объекты по уровню опасности обнаруженного вредоносного ПО:
 - Нажмите на заголовок столбца **Уровень опасности**.
 - Выберите уровни опасности.
8. Если требуется фильтровать объекты по результатам поведенческого анализа:
 - Нажмите на заголовок столбца **Поведенческий анализ**.
 - Выберите результаты поведенческого анализа.
9. Если требуется фильтровать объекты по другим столбцам, настройте фильтрацию аналогичным образом.

Фильтр объектов настроен, в таблице отображаются объекты, которые удовлетворяют всем указанным параметрам.

Поиск объектов с помощью языка запросов QL

- Чтобы найти объекты с помощью QL-запроса:

1. В главном меню выберите **Объекты**.
2. Включите режим ввода QL-запросов.
3. Введите запрос, используя [синтаксис языка запросов QL \(см. приложение Д\)](#).

Например:

```
age < 30d AND (correlated.state != UNKNOWN AND correlated.verdict.threat.classification IN ("TROJAN"))
```

4. Нажмите клавишу Enter.

В таблице появятся объекты, которые удовлетворяют QL-запросу.

Сохранение фильтра по объектам

Сохраненные вами фильтры не видны другим пользователям PT Email Security.

► Чтобы сохранить фильтр объектов:

1. В главном меню выберите **Объекты**.
2. Настройте фильтр по объектам.
3. В панели инструментов нажмите  → **Сохранить как новый**.
4. Введите название фильтра и нажмите кнопку **Создать**.

Сохранение отчета по объектам

Вы можете сохранить отчет по проверенным объектам в формате CSV. Отчет будет содержать информацию об отфильтрованных в таблице объектах.

► Чтобы сохранить отчет по объектам:

1. В главном меню выберите **Объекты**.
2. Настройте фильтр по объектам.
3. Нажмите кнопку **Скачать отчет**.

Файл отчета с названием `artifacts-<Дата и время скачивания>Z.csv` сохранен на ваш компьютер.

10.3. Работа с карточкой задания

Информация об обнаруженных в задании угрозах и вынесенном по заданию вердикте отображается в карточке задания. Страница карточки задания открывается щелчком мыши по названию задания на странице **Задания**.

Карточка задания содержит карточки отдельных объектов, проверенных в ходе выполнения этого задания. Страница карточки объекта открывается из карточки задания или щелчком мыши по названию объекта на странице **Объекты**.

Задание: payload.cs

Решение о блокировке: ☐ Не требуется **Вердикт: Бэкдор** **Уровень опасности:** 🔥🔥🔥 **Статус проверки:** ✓ Завершена

Дата создания: 23 июня, 10:29 [Детали](#)
 Источник: Веб-интерфейс
 Пользователь: Administrator

HTTP-заголовки

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/137.0.0.0 Safari/537.36
 Referer: https://10.120.6.100/tasks?progressStatus=FULL&progressStatus=UNSCANNED&progressStatus=PARTIAL&progressStatus=UNKNOWN&periodId=7d&sort=%7B%22start%22:%22desc%22%7D

Дочерние объекты

☒ Исключить угрозы с наследуемыми вердиктами [Сбросить](#)

Объект	Тип объек...	Вердикт	Причина верди...	Объект получен	У...	Метки	SHA-256
payload.cs	Файл	Бэкдор	Проверка PT ESC	От источника	🔥🔥🔥		27c1066fb...

[Скачать](#)

Рисунок 8. Карточка задания

В левой части страницы расположена панель для выбора объектов задания. В панели расположены:

- Блок поиска и фильтрации. В этом блоке вы можете искать объекты через обычный поиск или с помощью языка запросов QL. Здесь вы также можете отфильтровать объекты, используя следующие кнопки:

Показать только объекты поведенческого анализа;

Показать непроверенные объекты;

Показать частично проверенные объекты;

Показать потенциально опасные объекты;

Показать опасные объекты.

- Иерархический список объектов задания. При выборе в списке пункта **Задание**, открывается карточка задания. При выборе одного из объектов задания открывается карточка этого объекта. При выборе в списке для файла пункта **Поведенческий анализ**, открывается карточка поведенческого анализа файла. При выборе процесса, инициированного в ходе поведенческого анализа, этот процесс выделяется на диаграмме поведенческого анализа.
- Кнопка **Скачать**, которая позволяет скачивать из хранилища файлы, связанные с заданием на проверку.

Примечание. Вы можете скрывать и раскрывать панель по кнопке

Наполнение рабочей области зависит от выбранного в иерархическом списке элемента.

Карточка задания

При выборе в иерархическом списке задания в рабочей области отображаются несколько блоков параметров.

В верхней части рабочей области отображается:

- Название задания.
- Кнопка **i** с раскрывающимся списком для скачивания файлов и результатов проверки задания для анализа ложных срабатываний (недоступна для ссылок).
- Кнопка **Отчет по заданию** для выпуска отчета по заданию.

Для заблокированных и помещенных в карантин писем, отображается панель для работы с карантином:

- В верхней части панели отображается статус карантина. По ссылке **История карантина** вы можете просмотреть список событий, связанных с письмом в карантине.
- Кнопки для обработки писем в карантине:
 - **Выпустить из карантина** — для выпуска письма из карантина. Письмо будет отправлено получателям, указанным в письме (недоступна для удаленных писем).
 - **Переадресовать** — для отправки письма указанным вами получателям (недоступна для удаленных писем).
 - **Изменить информацию** — для изменения отметки о просмотре письма, даты удаления из карантина или комментария.
 - **Добавить комментарий** — для добавления комментария к письму.
 - **Удалить** — для удаления письма из карантина. После удаления письма его нельзя будет отправить получателям.
- В нижней части панели отображается информация о работе с письмом в карантине:
 - **Просмотрено** — отметка о просмотре письма в карантине (недоступна для удаленных писем). Вы можете установить постоянную или временную отметку о просмотре при выпуске, переадресации или изменении информации о письме.
 - **Выпущено** — количество получателей выпущенного из карантина письма. Если не удалось отправить письмо всем получателям, дополнительно отображается информация об ошибке и количество получателей, которым письмо было отправлено.
 - **Переадресовано** — количество получателей переадресованного письма. Если не удалось отправить письмо всем получателям, дополнительно отображается информация об ошибке и количество получателей, которым письмо было отправлено.
 - **Дата приема** — дата и время получения письма от источника.

- **Дата обновления информации** — дата последнего действия с письмом (недоступна для удаленных писем).
- **Комментарий** — комментарий к письму (недоступна для удаленных писем).
- **Получатели (SMTP)** — получатели письма.

В блоке с результатами проверки отображаются:

- **Решение о блокировке** — решение о допуске объекта задания в информационную систему организации.
- **Вердикт** — тип обнаруженного в задании вредоносного ПО.
- **Уровень опасности** — уровень опасности обнаруженного вредоносного ПО.
- **Статус проверки** — информация о ходе выполнения задания.

В блоке со свойствами задания отображаются:

- Общая информация о задании: дата создания, источник, с которого была инициирована проверка, пользователь, который запустил проверку.

По ссылке **Детали** отображаются не только дата и время создания задания, но и время обработки объекта задания источником (например, при блокировке объекта) и время вынесения вердикта по заданию.

- Дополнительная информация об источнике:
 - При проверке через веб-интерфейс PT Email Security — HTTP-заголовки (User-Agent, Referer).
 - Для почтовых источников — SMTP-адреса (откуда, куда).

Для заданий на проверку писем в блоке отображаются ссылки:

- **Детали обработки МТА** — ссылка для просмотра [карточки обработки письма почтовым транспортным агентом \(см. раздел 10.5\)](#). Ссылка доступна, если письмо получено от источника, поддерживающего работу с агентом.
- **Показать детали доставки** — ссылка для просмотра информации о доставке письма SMTP-сервером. Ссылка доступна, если выполнялись попытки отправки письма.
- **События по письму** — ссылка для просмотра всех [зарегистрированных для письма событий \(см. раздел 10.6\)](#).

В нижней части рабочей области отображается таблица **Дочерние объекты**. В таблице отображаются:

- На вкладке **Угрозы** — все объекты с угрозами. Если требуется, вы можете отключить отображение угроз с наследуемыми вердиктами, установив соответствующий флажок.

Вы можете отфильтровать объекты в таблице, а также просмотреть информацию о вердикте, нажав . При нажатии на название объекта открывается его карточка, в которой вы можете просмотреть информацию о проверке объекта.

- На вкладке **Все объекты** — все объекты задания. Если требуется, вы можете включить отображение только дочерних объектов первого уровня, установив соответствующий флажок.

Карточка объекта

При выборе в иерархическом списке объекта в рабочей области отображаются несколько блоков параметров.

В верхней части рабочей области отображаются:

- Название и тип объекта.
- Кнопка  для повторной проверки объекта (недоступна для HTTP-сообщений).
- Кнопка  с раскрывающимся списком для скачивания файлов и результатов проверки объекта для анализа ложных срабатываний (недоступна для ссылок).
- Кнопка  для копирования ссылки (доступна только для ссылок).
- Кнопка **Отчет по заданию** для выпуска отчета по заданию.

В блоке с результатами проверки отображаются:

- **Вердикт по объекту** — тип обнаруженного вредоносного ПО.
- **Уровень опасности** — уровень опасности обнаруженного вредоносного ПО.
- **Статус проверки** — статус проверки объекта.

В блоке со свойствами объекта отображаются:

- Метки объекта, указывающие на [особенности файла или тематику ресурса, на который ведет ссылка \(см. приложение Г\)](#).
- Свойства объекта:
 - Для файла и тела письма — хеш-суммы (SHA-256, SHA-1, MD5, SSDEEP), размер, MIME-тип, формат и дополнительная информация о содержимом.
 - Для письма — адреса из заголовков From, To, CC, BCC и тема.

Примечание. По ссылкам **Показать** и **HTML-версия** вы можете просмотреть сообщение письма в виде простого текста или в HTML-формате. По ссылке **Все заголовки** вы можете просмотреть все заголовки письма и при необходимости скопировать их или скачать в виде файла.

- Для ссылки — исходная ссылка, цепочка переадресаций с кодом ответа (если выполнялась переадресация), средство проверки, с помощью которого ссылка была обработана, и код ответа на HTTP-запрос по ссылке.
 - Для HTTP-сообщения — HTTP-заголовки запроса или ответа.
- Ссылка **Найти объект в других заданиях** для поиска заданий, в которых ранее проверялся этот объект.
 - Ссылка **Искать в базе VirusTotal** для поиска хеш-суммы объекта в базе VirusTotal.
 - Ссылка **Искать в базе IoC Portal** для перехода на PT IoC Portal, где можно посмотреть дополнительную информацию об индикаторе компрометации.

Примечание. Для создания учетной записи на PT IoC Portal вы можете обратиться в техническую поддержку Positive Technologies.

В рабочей области отображаются блоки с результатами проверки различными методами:

- **Черный и белый списки** — информация о том, находились ли хеш-суммы объекта в черном или белом списке на момент проверки. Нажав на ссылку **Найти файл в списках**, вы можете обновить информацию о нахождении объекта в списках, а также добавить его в черный или белый список.
- **Статический анализ** — результаты проверки с помощью антивирусов, по индикаторам компрометации и экспертным YARA-правилам.
- **Пользовательские средства проверки** — результаты проверки по пользовательским YARA-правилам.
- **Дополнительные критерии** — результаты проверки по пользовательским правилам определения файлов и ссылок с угрозами.
- **Защита от угроз в почте** — результаты проверки по спискам DNS-блокировок.
- **Поведенческий анализ** — результаты поведенческого анализа.

Если выбранный объект содержит дочерние объекты, в нижней части рабочей области отображается таблица **Дочерние объекты**. В таблице отображаются:

- На вкладке **Угрозы** — все объекты с угрозами. Если требуется, вы можете отключить отображение угроз с наследуемыми вердиктами, установив соответствующий флажок.

Вы можете отфильтровать объекты в таблице, а также просмотреть информацию о вердикте, нажав ⓘ. При нажатии на название объекта открывается его карточка, в которой вы можете просмотреть информацию о проверке объекта.

- На вкладке **Все объекты** — все объекты задания. Если требуется, вы можете включить отображение только дочерних объектов первого уровня, установив соответствующий флажок.

Выпуск отчета по заданию

Из карточки задания вы можете сформировать отчет с результатами выполнения задания. В отчет добавляется основная информация о задании и обнаруженных угрозах.

► Чтобы выпустить отчет по заданию:

1. В главном меню выберите **Задания**.
2. Щелчком мыши по названию задания откройте карточку задания.
3. Нажмите кнопку **Отчет по заданию**.

Откроется окно браузера для настройки печати.

4. Настройте формат выпуска отчета и выпустите его.

В зависимости от выбранных параметров отчет сохранен на компьютере или отправлен на печать.

Обработка писем в карантине

Письма, заблокированные по результатам проверки, могут быть помещены в карантин. Рекомендуется отслеживать появление новых писем в карантине, регулярно их обрабатывать и своевременно принимать решение об их опасности. При обработке письма вы можете выпустить его из карантина, переслать, изменить срок хранения, добавить к нему комментарий или удалить его. Обработанные письма помечаются как просмотренные.

Примечание. Для отслеживания появления новых писем в карантине и регулярной обработки таких писем предназначена страница **Карантин**.

► Чтобы обработать письмо в карантине:

1. В главном меню выберите **Задания**.

Примечание. Для поиска заданий с письмами в карантине вы можете добавить в таблицу столбец **Решение о блокировке** и выбрать для него значение **Заблокировать** и столбец **Карантин** и выбрать для него статус **В карантине**.

2. Щелчком мыши по названию задания откройте карточку задания для письма в карантине.
3. Если вы считаете письмо безопасным:
 - В панели для работы с карантином нажмите кнопку **Выпустить из карантина**.
 - Если требуется, измените отметку о просмотре письма.
 - В поле **Комментарий** введите любой текстовый комментарий.
 - Нажмите кнопку **Выпустить**.
4. Если вы хотите переслать письмо другим получателям:
 - В панели для работы с карантином нажмите **Переадресовать**.

- В открывшемся окне в поле **Получатели (SMTP)** введите адреса электронной почты.
 - Если требуется, измените отметку о просмотре письма.
 - В поле **Комментарий** введите любой текстовый комментарий.
 - Нажмите кнопку **Отправить**.
5. Если вы хотите отложить принятие решения по письму:
- В панели для работы с карантином нажмите **Изменить информацию**.
 - В открывшемся окне отметьте письмо как просмотренное.
 - Установите флажок **Временно отметить до** и введите дату.
 - Если необходимо, в поле **Дата удаления из карантина** измените дату.
 - В поле **Комментарий** введите любой текстовый комментарий.
 - Нажмите кнопку **Изменить**.
6. Если вы считаете письмо опасным:
- В панели для работы с карантином нажмите **Изменить информацию**.
 - В открывшемся окне отметьте письмо как просмотренное.
 - Если необходимо, в поле **Дата удаления из карантина** измените дату удаления письма.
 - В поле **Комментарий** введите любой текстовый комментарий.
 - Нажмите кнопку **Изменить**.
7. Если вы считаете письмо опасным и хотите его удалить:
- В панели для работы с карантином нажмите **Удалить**.
 - В открывшемся окне в поле **Комментарий** введите любой текстовый комментарий.
 - Нажмите кнопку **Удалить**.

Добавление файла в черный или белый список

- Чтобы добавить файл в черный или белый список из карточки объекта:
1. В главном меню выберите **Объекты**.
 2. Щелчком мыши по названию объекта откройте карточку объекта.
 3. В блоке **Черный и белый списки** по ссылке **Найти файл в списках** запустите поиск.
 4. В открывшемся окне нажмите кнопку **Добавить в черный список** или **Добавить в белый**.
 5. Нажмите кнопку **Добавить**.

Перемещение файлов между списками

► Чтобы переместить файл из одного списка в другой:

1. В главном меню выберите **Объекты**.
2. Щелчком мыши по названию объекта откройте карточку объекта.
3. В блоке **Черный и белый списки** по ссылке **Найти файл в списках** запустите поиск.
4. В открывшемся окне нажмите кнопку **Переместить в черный список** или **Переместить в белый список**.

Повторная проверка объекта

► Чтобы запустить повторную проверку объекта:

1. В главном меню выберите **Объекты**.
2. Щелчком мыши по названию объекта откройте карточку объекта.
3. Нажмите .
4. Настройте параметры проверки объекта.

Для объекта создано новое задание на проверку.

10.4. Работа с карточкой поведенческого анализа

Результаты поведенческого анализа доступны для файла, если поведенческий анализ поддерживается для этого типа файлов и в параметрах проверки файла был включен поведенческий анализ. Вся информация, полученная в ходе анализа поведения файлов и все созданные при этом артефакты, отображаются в карточке поведенческого анализа.

Открыть карточку поведенческого анализа можно через раздел **Объекты** главного меню, выбрав в столбце **Тип элемента в структуре задания** значение **Карточка поведенческого анализа**, или через раздел **Задания**, выбрав задание, для которого был проведен поведенческий анализ.

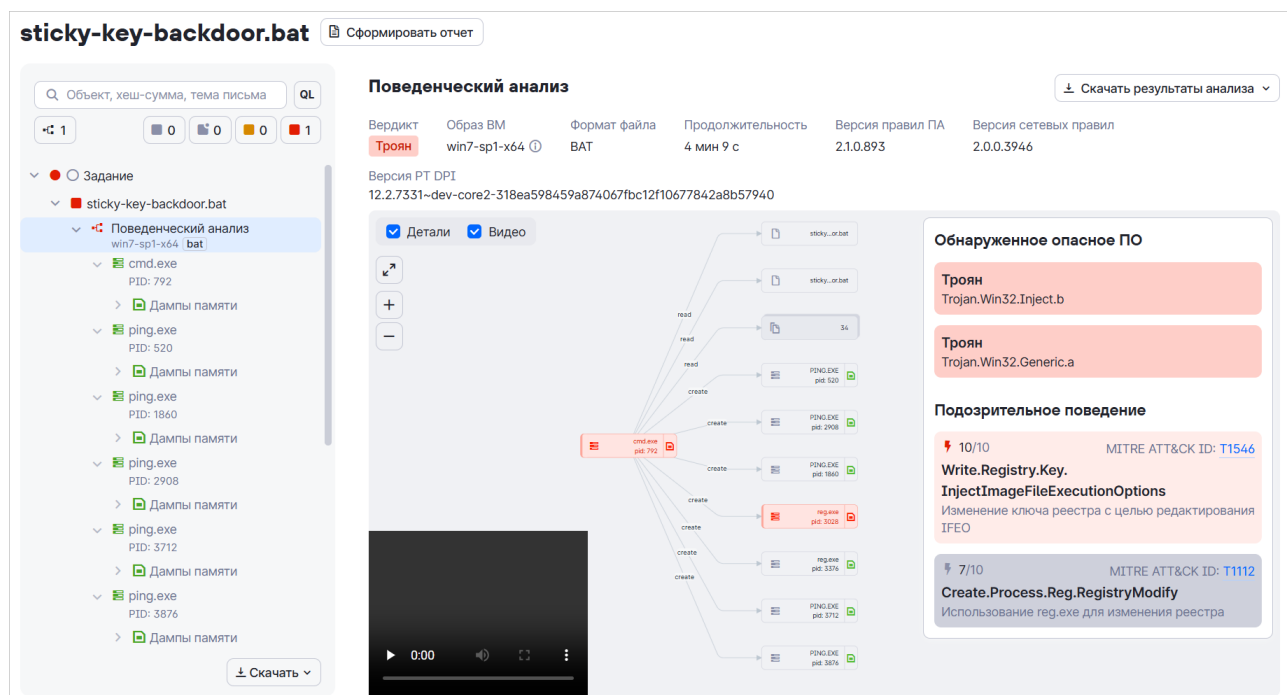


Рисунок 9. Карточка поведенческого анализа

В левой части страницы расположена панель для выбора объектов задания. В панели расположены:

- Блок поиска и фильтрации. В этом блоке вы можете искать объекты через обычный поиск или с помощью языка запросов QL. Здесь вы также можете отфильтровать объекты, используя следующие кнопки:

-  Показать только объекты поведенческого анализа;
-  Показать непроверенные объекты;
-  Показать частично проверенные объекты;
-  Показать потенциально опасные объекты;
-  Показать опасные объекты.

- Иерархический список объектов задания. При выборе в списке пункта **Задание**, открывается карточка задания. При выборе одного из объектов задания открывается карточка этого объекта. При выборе в списке для файла пункта **Поведенческий анализ**, открывается карточка поведенческого анализа файла. При выборе процесса, инициированного в ходе поведенческого анализа, этот процесс выделяется на диаграмме поведенческого анализа.
- Кнопка **Скачать**, которая позволяет скачивать из хранилища файлы, связанные с заданием на проверку.

Примечание. Вы можете скрывать и раскрывать панель по кнопке .

В верхней части рабочей области страницы указана информация о поведенческом анализе: вердикт по файлу, образ VM, формат файла, продолжительность наблюдения за файлом, версия правил поведенческого анализа, версия правил для проверки сетевых пакетов и средства проверки PT DPI.

Также тут расположена кнопка **Скачать результаты анализа**, нажав которую вы можете выбрать, какие файлы с результатами нужно скачать:

- `events-correlated.log.gz` — содержит корреляционные события в формате JSON. События регистрируются на основании правил корреляции при анализе нормализованных событий и содержат информацию о выявленном опасном и потенциально опасном поведении файла.
- `tcpdump.pcap` — содержит копию сетевого трафика в формате PCAP.
- `events-normalized.log.gz` — содержит нормализованные события в формате JSON.
- `drakvuf-trace.log.gz` — содержит зарегистрированные при анализе поведения файла события в формате простого текста.

В центральной части рабочей области страницы расположена диаграмма поведенческого анализа, панель с результатами поведенческого анализа файла и окно для просмотра видеозаписи поведения файла.

Примечание. Вы можете скрыть панель с результатами поведенческого анализа файла и окно для просмотра видеозаписи поведения файла, сняв флажки **Детали** и **Видео**.

Диаграмма поведенческого анализа

На диаграмме показана последовательность действий, которые файл выполнял в операционной системе. Действия, произошедшие раньше, на диаграмме располагаются левее. Прямоугольниками на диаграмме обозначены объекты. Стрелки показывают связи между объектами: создание, изменение, чтение данных или удаление. При выборе объекта вы можете посмотреть информацию об объекте.

Примечание. Вы можете увеличить масштаб диаграммы двойным щелчком мыши и управлять масштабом диаграммы, используя колесо мыши или кнопки **+** и **−**. Для удобства просмотра вы можете расширить область диаграммы, нажав . При повторном нажатии область диаграммы примет прежний размер.

На диаграмме могут отображаться следующие типы объектов:

 — процесс (если для процесса проверялся дамп памяти, то для объекта также отображается значок 

 — файл или группа файлов;

 — обращение к реестру или группе реестров;

 — служба;

IP — IP;



— сокет;

URL — сервер или гиперссылка;



— сетевой пакет;



— мьютекс;



— именованный канал;



— точка соединения, жесткая ссылка или символическая ссылка.

Панель с результатами поведенческого анализа

В панели вы можете просмотреть информацию о выбранном объекте диаграммы. Если объект на диаграмме не выбран, то отображается информация о результате поведенческого анализа, которая разделена на следующие блоки:

- Блок **Результат поведенческого анализа**. В этом блоке отображается конечный результат поведенческого анализа — тип обнаруженной угрозы.
- Блок **Обнаруженное опасное ПО**. Блок отображается, если было обнаружено вредоносное ПО. В блоке для каждого такого ПО отображается его тип и название в формате `<Class>.<Platform>.<Family>.<Modification>`, где:
 - `<Class>` — класс вредоносного ПО (например, Trojan, Backdoor, Hacktool);
 - `<Platform>` — платформа или файл, в котором обнаружено вредоносное ПО (например, Win32, Java, VBS);
 - `<Family>` — семейство вредоносного ПО или название инструмента (например, HyperBro, Kazuar, Flame);
 - `<Modification>` — модификация вредоносного ПО (например, a, b, c).

Примечание. Вы можете скопировать название обнаруженного вредоносного ПО, двойным щелчком мыши.

- Блок **Опасные сетевые объекты**. Блок отображается, если было обнаружено обращение к сетевым объектам и по индикаторам компрометации эти объекты были определены как опасные. Для каждого объекта отображается тип ВПО, индикатор компрометации и тип индикатора (**byDomain** — домен, **byIp** — IP-адрес, **byUrl** — ссылка). Также для объекта отображается ссылка для перехода на IoC Portal, где можно найти дополнительную информацию об индикаторе компрометации.

Примечание. Для создания учетной записи на IoC Portal вы можете обратиться в техническую поддержку Positive Technologies.

- Блок **Сетевые атаки**. Блок отображается, если при анализе сетевых пакетов средством проверки PT DPI были обнаружены признаки атаки. Для каждой атаки отображается ее название, описание и идентификатор.
- Блок **Подозрительное поведение**. В этом блоке по каждому обнаруженному подозрительному поведению отображается его название, уровень опасности и идентификатор техники MITRE ATT&CK, нажав на который можно перейти на сайт MITRE ATT&CK на страницу с информацией о технике. Для названия подозрительного поведения используется формат `<Action>.<Object>.<Property>.<Description>`, где:
 - `<Action>` — выполняемое действие (например, Create, Write, Delete);
 - `<Object>` — объект, над которым выполняется действие (например, Process, Registry, File);
 - `<Property>` — свойство объекта, на которое направлено действие (например, Attribute, Data, Key);
 - `<Description>` — дополнительная информация об обнаруженном опасном действии файла (например, Persistence, Evasion, UACBypass).

Окно просмотра видеозаписи поведения файла

Окно предназначено для просмотра видеозаписи поведения файла в ОС. Видеозапись недоступна, если в параметрах проверки файла была отключена запись видео. В окне доступны кнопки для запуска ► и остановки || воспроизведения, для разворачивания окна на весь экран [] и его сворачивания []. По кнопке ⋮ вы можете скачать видеозапись, настроить скорость воспроизведения и перейти в режим просмотра «картинка в картинке».

Скачивание результатов поведенческого анализа

Для режима проверки с перезагрузкой операционной системы результаты поведенческого анализа необходимо скачивать отдельно до перезагрузки и после нее. Этот режим доступен только при проверке объектов через веб-интерфейс.

- Чтобы скачать результаты поведенческого анализа:
 1. В главном меню выберите **Задания**.
 2. Щелчком мыши в строке таблицы откройте карточку задания.
 3. В панели слева выберите **<Название файла> → Поведенческий анализ**.
 4. Нажмите кнопку **Скачать результаты анализа**.
 5. Отметьте нужные вам файлы и нажмите кнопку **Скачать**.

Результаты поведенческого анализа добавлены в архив `sandbox_logs.zip` и скачаны на ваш компьютер.

10.5. Просмотр очереди обработки писем МТА

Для работы с письмами, полученными от источников типа «Почтовый сервер в режиме фильтрации (МТА)» и «Почтовый шлюз безопасности», используется встроенный в PT Email Security почтовый транспортный агент.

Для просмотра очереди обработки писем почтовым транспортным агентом предназначена страница **Письма** → **Очередь обработки МТА**.

Письма / Очередь обработки МТА

* По умолчанию ↶ ● Режим QL-запросов ⚙️ 🔍

Отправить недоставленные письма

☐	Дата при...	↑	Карант...	Оригинал письма	Тема	Отправите...	Получатели (S...	Статус обработ... 3 значения	Источник	↑	Идентификатор...	Размер пи...	↓
☐	25 ноя, 04:23:2...			Доставлен	test#1-49	sender@test.ru	recipient1@test....	Обработано	test-mta		#id:953c0625-b...	871 Б	
☐	25 ноя, 04:23:2...			Доставлен	test#1-51	sender@test.ru	recipient1@test....	Обработано	test-mta		#id:eece2dd2-3...	871 Б	
☐	25 ноя, 04:23:2...			Доставлен	test#1-52	sender@test.ru	recipient1@test....	Обработано	test-mta		#id:0ff898a0-1d...	871 Б	
☐	25 ноя, 04:23:2...			Доставлен	test#1-54	sender@test.ru	recipient1@test....	Обработано	test-mta		#id:ca1a2734-6...	871 Б	
☐	25 ноя, 04:23:2...			Доставлен	test#1-53	sender@test.ru	recipient1@test....	Обработано	test-mta		#id:db654c80-8...	871 Б	
☐	25 ноя, 04:23:2...			Доставлен	test#1-56	sender@test.ru	recipient1@test....	Обработано	test-mta		#id:f2dbf827-4d...	871 Б	
☐	25 ноя, 04:23:2...			Доставлен	test#1-55	sender@test.ru	recipient1@test....	Обработано	test-mta		#id:33cac44a-3...	871 Б	
☐	25 ноя, 04:23:2...			Доставлен	test#1-57	sender@test.ru	recipient1@test....	Обработано	test-mta		#id:b821ff95-09...	871 Б	
☐	25 ноя, 04:23:2...			Доставлен	test#1-58	sender@test.ru	recipient3@test....	Обработано	test-mta		#id:13988a45-f9...	871 Б	

Всего 300 1 2 3 4 5 6 < >

Рисунок 10. Страница **Очередь обработки МТА**

В панели инструментов страницы расположены:

- Кнопка **<Название фильтра>** для выбора фильтра. По кнопке раскрывается меню, в котором вы можете выбрать один из сохраненных фильтров или фильтр по умолчанию. В верхней части меню доступно поле для быстрого поиска фильтра.
- Кнопка **⋮** для выбора дополнительных действий с фильтром. После настройки параметров фильтрации по этой кнопке вы можете сохранить их как новый фильтр или сбросить все изменения. После изменения параметров созданного ранее фильтра по этой кнопке вы можете сохранить для него измененные параметры фильтрации, сохранить параметры фильтрации как новый фильтр, сбросить все изменения, переименовать фильтр или удалить его.
- Кнопка **↶** для выбора фильтра по умолчанию.
- Переключатель **Режим QL-запросов** для создания фильтра с помощью языка запросов QL. В этом режиме появляется поле для ввода QL-запросов, кнопки **<** и **>** для выбора предыдущего или следующего запроса и кнопка **🕒** для просмотра списка выполненных ранее запросов.
- Кнопка **⚙️** для выбора столбцов, которые должны отображаться в таблице.

- Кнопка  для обновления данных в таблице.
- Кнопка  для настройки автоматического обновления данных в таблице.

Ниже расположена кнопка **Отправить недоставленные письма** для повторной отправки выбранных писем или повторной отправки всех писем, которые не были доставлены из-за ошибки доставки.

В рабочей области страницы расположена таблица со списком писем. Вы можете фильтровать письма в таблице по столбцам или с помощью QL-запроса.

В зависимости от вашего выбора таблица может содержать следующие столбцы с информацией о письмах:

- **Дата приема** — дата и время получения письма от источника. По умолчанию в таблице отображаются письма за последние 7 дней.
- **Карантин** — помещено ли письмо в карантин.
- **Оригинал письма** — действие с оригиналом письма:
 - **Доставлен** — письмо доставлено всем получателям.
 - **Доставлен не всем** — письмо не доставлено некоторым получателям.
 - **Не доставлен** — письмо не доставлено ни одному из получателей.
- **Тема** — тема письма. По ссылке в столбце вы можете открыть карточку с деталями обработки письма.
- **Отправитель (SMTP)** — электронный адрес отправителя письма.
- **Получатель (SMTP)** — электронные адреса получателей письма.
- **Статус обработки:**
 - **В очереди** — письмо принято, но обработка письма не начата.
 - **Обрабатывается** — в зависимости от параметров проверки письмо отправляется на проверку, отправляется получателям или блокируется.
 - **Обработано** — обработка письма завершена.
 - **Ошибки** — при работе с письмом возникли ошибки: **Не удалось доставить**, **Не удалось проверить**, **Не удалось сохранить в карантине** или **Неудачная попытка доставки**.
- **Источник** — источник, от которого получено письмо.
- **Идентификатор (Message-ID)** — идентификатор письма.
- **Размер письма**.

Карточка обработки письма МТА

Страница карточки обработки письма МТА открывается щелчком мыши по теме письма в таблице на странице **Очередь обработки МТА** или по ссылке **Детали обработки МТА** в карточке задания на проверку письма.

В заголовке карточки указана тема письма. В верхней части карточки указаны дата приема письма, статус обработки письма, отправитель и получатели письма, полученные от SMTP-сервера.

В рабочей области карточки расположены вкладки:

- **Информация** — содержит общую информацию о принятом письме: в блоке **Прием** — детали приема письма, в блоке **Заголовки** — заголовки письма, в блоке **Вложения** — таблица со списком вложенных файлов.
- **Решения по получателям** — содержит таблицу со списком действий, которые выполнены с письмом в зависимости от получателя. Решение о том какое действие будет выполнено зависит от того какое правило обработки письма было применено для получателя.
- **Исходящие по письму** — содержит таблицу со списком получателей, которым было отправлено письмо и информацией о доставке. По кнопке **Отправить недоставленные письма** вы можете повторно отправить письмо получателям в таблице, которым оно не было доставлено из-за ошибки доставки.
- **События по письму** — содержит таблицу со списком событий по письму.

10.6. Просмотр событий по письмам

Вы можете просматривать события, связанные с письмами, полученными от источников типа «Почтовый сервер в режиме фильтрации», «Почтовый сервер в режиме зеркалирования» и «Сервер Microsoft Exchange с установленным агентом». Отображаются события, связанные с приемом и отправкой писем, взаимодействием с SMTP-сервером, применением правил обработки писем, их последующей обработкой и проверкой, вынесением вердикта, а также с действиями с письмами в карантине. Для просмотра событий предназначена страница **Письма** → **События по письмам**.

* По умолчанию ↶ ● Режим QL-запросов ⚙️ 🔍 ⋮						
Дата	↓	Событие	⇒	Метки	Важность	Источник 3 значения
15 окт, 16:39:43,134		('10.120.7.129', 33771) << b'250 OK id=424e3416-a9b3-11f0-800d-816a0f9b12...		Прием	Информация	mail-gateway...
15 окт, 16:39:43,133		Email processing completed successfully		Прием	Информация	mail-gateway...
15 окт, 16:39:43,126		Email send: <SMTPSender mail_from="user1@domain1.com" recipients=["user...		Отправка	Информация	mail-gateway...
15 окт, 16:39:42,953		SMTP-connection from ('10.244.127.43', 38702) to ('10.120.7.129', 31109) is esta...		Отправка	Информация	mail-gateway...
15 окт, 16:39:42,952		('10.120.7.129', 31109) >> 220 checkme.lab ESMTP Postfix (Ubuntu)		Отправка	Информация	mail-gateway...
15 окт, 16:39:42,822		Email is trying to send: <SMTPSender mail_from="user1@domain1.com" recipi...		Отправка	Информация	mail-gateway...
15 окт, 16:39:42,821		Original message <176052478149.115177934491849720186@domain1.com> w...		Обработка	Информация	mail-gateway...
15 окт, 16:39:42,821		Email is CLEAN		Обработка	Информация	mail-gateway...
Всего 129				1 2 3 < >		

Рисунок 11. Страница **События по письмам**

В панели инструментов страницы расположены:

- Кнопка **<Название фильтра>** для выбора фильтра. По кнопке раскрывается меню, в котором вы можете выбрать один из сохраненных фильтров или фильтр по умолчанию. В верхней части меню доступно поле для быстрого поиска фильтра.
- Кнопка **⋮** для выбора дополнительных действий с фильтром. После настройки параметров фильтрации по этой кнопке вы можете сохранить их как новый фильтр или сбросить все изменения. После изменения параметров созданного ранее фильтра по этой кнопке вы можете сохранить для него измененные параметры фильтрации, сохранить параметры фильтрации как новый фильтр, сбросить все изменения, переименовать фильтр или удалить его.
- Кнопка **↶** для выбора фильтра по умолчанию.
- Переключатель **Режим QL-запросов** для создания фильтра с помощью языка запросов QL. В этом режиме появляется поле для ввода QL-запросов, кнопки **<** и **>** для выбора предыдущего или следующего запроса и кнопка **🕒** для просмотра списка выполненных ранее запросов.
- Кнопка **⚙️** для выбора столбцов, которые должны отображаться в таблице.
- Кнопка **🔄** для обновления данных в таблице.
- Кнопка **⋮** для настройки автоматического обновления данных в таблице.

В рабочей области страницы расположена таблица со списком событий, связанных с письмами. Вы можете фильтровать события в таблице по столбцам или с помощью QL-запроса. При наведении курсора на строку таблицы в ней появляются:

- Ссылка **Письмо** для просмотра [карточки обработки письма почтовым транспортным агентом \(см. раздел 10.5\)](#). Ссылка доступна, если письмо получено от источника, поддерживающего работу с агентом.
- Ссылка **Задание** для просмотра карточки задания. Ссылка доступна, если для письма уже создано задание на проверку.
- Кнопка **Связанные события** для просмотра в новом окне всех событий, связанных с письмом.

В зависимости от вашего выбора таблица может содержать следующие столбцы с информацией о событии:

- **Дата** — дата и время регистрации события. По умолчанию в таблице отображаются события за последние 7 дней.
- **Событие** — текст события. С помощью кнопок  и  в заголовке столбца вы можете включать и отключать перенос строк текста события.
- **Метки** — метки события. Предусмотрены метки: **Прием, Обработка, Отправка и Карантин**.
- **Важность** — важность события. Предусмотрены уровни важности: **Информация, Предупреждение и Ошибка**.
- **Источник** — название источника, от которого получено событие.

Просмотр связанных событий

Вы можете просмотреть все события, которые связаны с тем же письмом, что и событие, выбранное в таблице.

► Чтобы просмотреть связанные события:

1. В главном меню выберите **Письма** → **События по письмам**.
2. Наведите курсор на строку таблицы и нажмите кнопку **Связанные события**.

Откроется окно **Связанные события по письму: <Тема письма>**.

10.7. Работа с письмами в карантине

Письма, заблокированные по результатам проверки, могут быть помещены в карантин. Рекомендуется отслеживать появление новых писем в карантине, регулярно их обрабатывать и своевременно принимать решение об их опасности. При обработке письма вы можете выпустить его из карантина, переслать, изменить срок хранения, добавить к нему комментарий или удалить его. Обработанные письма помечаются как просмотренные.

Для работы с письмами в карантине предназначена страница **Письма** → **Карантин**.

По умолчанию

Режим QL-запросов

Выпустить из карантина

Переадресовать

Изменить информацию

Добавить комментарий

Удалить

Дата пр... За после...	Карантин	Письмо	Просмотрено	Выпущено	Переадресовано	Комментарий	Будет удалено В любое время	Дата обновления... За все время	Вердикт при блокировке
23 июля, 12:3...	Удалено	EICA		1			23 июля, 12:36:04	Вирус	
23 июля, 14:0...	В карантине	EICA				22 авг, 14:07	22 авг, 14:30	Нет результата	
23 июля, 14:3...	В карантине	EICA				22 авг, 14:30	22 авг, 14:30	Нет результата	
24 июля, 20:4...	Выпущено	EICA		1		23 авг, 20:47	24 июля, 20:51:04	Вирус	
24 июля, 20:5...	Удалено	EICA		1		23 авг, 20:47	24 июля, 20:52:28	Вирус	
24 июля, 21:2...	В карантине	EICA				23 авг, 21:21	24 июля, 20:52:28	Нет результата	
25 июля, 10:1...	Выпущено	EICA		1	1	24 авг, 10:13	25 июля, 10:18:06	Вирус	
25 июля, 10:2...	В карантине	EICA			1 из 2	24 авг, 10:25	25 июля, 10:28:13	Вирус	

Всего 27

1

Рисунок 12. Страница **Карантин**

В панели инструментов страницы расположены:

- Кнопка **<Название фильтра>** для выбора фильтра. По кнопке раскрывается меню, в котором вы можете выбрать один из сохраненных фильтров или фильтр по умолчанию. В верхней части меню доступно поле для быстрого поиска фильтра.
- Кнопка **:** для выбора дополнительных действий с фильтром. После настройки параметров фильтрации по этой кнопке вы можете сохранить их как новый фильтр или сбросить все изменения. После изменения параметров созданного ранее фильтра по этой кнопке вы можете сохранить для него измененные параметры фильтрации, сохранить параметры фильтрации как новый фильтр, сбросить все изменения, переименовать фильтр или удалить его.
- Кнопка **↶** для выбора фильтра по умолчанию.
- Переключатель **Режим QL-запросов** для создания фильтра с помощью языка запросов QL. В этом режиме появляется поле для ввода QL-запросов, кнопки **<** и **>** для выбора предыдущего или следующего запроса и кнопка **🕒** для просмотра списка выполненных ранее запросов.
- Кнопка **⚙️** для выбора столбцов, которые должны отображаться в таблице.
- Кнопка **🔄** для обновления данных в таблице.
- Кнопка **:** для настройки автоматического обновления данных в таблице.

Ниже расположены кнопки для работы с выбранными в таблице письмами:

- **Выпустить из карантина** — для выпуска выбранных писем из карантина.

Примечание. Для выбора в таблице нескольких писем вы можете установить для них флажки в первом столбце, для выбора всех писем — установить флажок в заголовке первого столбца.

- **Переадресовать** — для отправки выбранных писем указанным вами получателям.
- **Изменить информацию** — для изменения у выбранных писем отметки о просмотре, даты удаления из карантина или комментария.
- **Добавить комментарий** — для добавления комментария к выбранным письмам.
- **Удалить** — для удаления выбранных писем из карантина.

В рабочей области страницы расположена таблица со списком писем, помещенных в карантин. Вы можете фильтровать письма в таблице по столбцам или с помощью QL-запроса.

При наведении курсора на строку таблицы в ней появляются кнопки для работы с отдельным письмом. По кнопке  вы можете выпустить письмо из карантина, по кнопке  — переадресовать письмо, по кнопке  — изменить информацию о письме, по кнопке  — добавить комментарий, по кнопке  — удалить письмо из карантина.

В зависимости от вашего выбора, таблица может содержать следующие столбцы с информацией о письме:

- **Дата приема** — дата и время получения письма от источника. По умолчанию в таблице отображаются письма за последние 7 дней.
- **Идентификатор письма** — идентификатор письма в PT Email Security.
- **Карантин** — статус письма в карантине:
 - **Помещается в карантин** — письмо помещается в карантин.
 - **Ошибка помещения в карантин** — не удалось поместить письмо в карантин.
 - **В карантине** — письмо в карантине.
 - **Выпускается из карантина** — письмо отправляется получателем.
 - **Выпущено** — письмо отправлено получателем.
 - **Удалено** — письмо удалено из карантина вручную или автоматически. Удаленное письмо отображается в таблице 30 дней.
- **Письмо** — тема письма.
- **Просмотрено** — отметка о просмотре письма. Вы можете установить постоянную или временную отметку о просмотре при выпуске, переадресации или изменении информации о письме.
- **Выпущено** — количество получателей выпущенного из карантина письма. Если не удалось отправить письмо всем получателям, дополнительно отображается информация об ошибке и количество получателей, которым письмо было отправлено.

- **Переадресовано** — количество получателей переадресованного письма. Если не удалось отправить письмо всем получателям, дополнительно отображается информация об ошибке и количество получателей, которым письмо было отправлено.
- **Комментарий** — комментарий к письму.
- **Будет удалено** — планируемая дата удаления письма из карантина. Определяется сроком хранения писем в карантине, но может быть изменена вручную.
- **Дата обновления информации** — дата последнего действия с письмом.
- **Вердикт при блокировке** — вердикт по заданию, на основании которого письмо помещено в карантин. Нажав [↗](#), вы можете открыть карточку задания.
- **Отправитель (SMTP)** — отправитель письма.
- **Получатели (SMTP)** — получатели письма.
- **Message-ID** — значение заголовка Message-ID.
- **Источник** — название источника, от которого письмо поступило на проверку.

Обработка письма в карантине

► Чтобы обработать письмо в карантине:

1. В главном меню выберите **Письма** → **Карантин**.

Примечание. Для поиска необработанных писем вы можете в столбце **Карантин** выбрать статус **В карантине**, а в столбце **Просмотрено** выбрать значение **Не просмотрено**.

2. В строке письма в столбце **Вердикт при блокировке** нажмите [↗](#).
В новой вкладке браузера откроется карточка задания.
3. Выполните необходимые действия с письмом.

Выпуск письма из карантина

Если вы считаете письмо безопасным, вы можете выпустить его из карантина, письмо будет отправлено указанным в нем получателям. Копия письма продолжит храниться в карантине до истечения срока хранения.

► Чтобы выпустить письмо из карантина:

1. В главном меню выберите **Письма** → **Карантин**.
2. Выберите письмо в таблице.
3. В панели инструментов нажмите кнопку **Выпустить из карантина**.
4. Если требуется, измените отметку о просмотре письма.

5. В поле **Комментарий** введите любой текстовый комментарий.
6. Нажмите кнопку **Выпустить**.

Переадресация письма

Если вы хотите отправить письмо получателям, которые не были в нем указаны, вы можете переадресовать письмо. Копия письма продолжит храниться в карантине до истечения срока хранения.

- ▶ Чтобы переадресовать письмо из карантина:
 1. В главном меню выберите **Письма** → **Карантин**.
 2. Выберите письмо в таблице.
 3. В панели инструментов нажмите кнопку **Переадресовать**.
 4. В поле **Получатели (SMTP)** введите адреса электронной почты получателей.
 5. Если требуется, измените отметку о просмотре письма.
 6. В поле **Комментарий** введите любой текстовый комментарий.
 7. Нажмите кнопку **Отправить**.

Изменение даты удаления письма из карантина

При необходимости вы можете изменить срок хранения, который был установлен для письма при его добавлении в карантин.

- ▶ Чтобы изменить дату удаления письма из карантина:
 1. В главном меню выберите **Письма** → **Карантин**.
 2. Выберите письмо в таблице.
 3. В панели инструментов нажмите кнопку **Изменить информацию**.
 4. Введите новую дату удаления письма из карантина.
 5. Если требуется, измените отметку о просмотре письма.
 6. В поле **Комментарий** введите любой текстовый комментарий.
 7. Нажмите кнопку **Изменить**.

Добавление комментария

- ▶ Чтобы добавить комментарий к письму в карантине:
 1. В главном меню выберите **Письма** → **Карантин**.
 2. Выберите письмо в таблице.

3. В панели инструментов нажмите кнопку **Добавить комментарий**.
4. В поле **Комментарий** введите любой текстовый комментарий.
5. Нажмите кнопку **Добавить**.

Удаление письма из карантина

Если вы считаете письмо опасным, вы можете удалить его из карантина раньше установленного срока хранения.

► Чтобы удалить письмо из карантина:

1. В главном меню выберите **Письма** → **Карантин**.
2. Выберите письмо в таблице.
3. В панели инструментов нажмите кнопку **Удалить**.
4. В поле **Комментарий** введите любой текстовый комментарий.
5. Нажмите кнопку **Удалить**.

10.8. Скачивание файлов из хранилища

В целях безопасности все скачиваемые из хранилища файлы помещаются в зашифрованный ZIP-архив с названием `Archive-<Идентификатор задания>-<Дата и время скачивания>Z.zip` и паролем `infected`.

Содержимое архива зависит от способа, который вы используете для скачивания файлов:

- Если вы скачиваете выбранный файл, в архив помещается только этот файл.
- Если вы скачиваете файлы, отфильтрованные в панели выбора объектов, в архив помещаются только отфильтрованные файлы.
- Если вы скачиваете все файлы задания, в архив помещаются все файлы, извлеченные при выполнении задания.
- Если вы скачиваете информацию о проверке выбранного файла для техподдержки, в архив помещается этот файл и его дочерние объекты.

Примечание. При необходимости вы можете скачать для техподдержки только результаты проверки файла или задания, не скачивая проверенные файлы.

- Если вы скачиваете информацию о проверке задания для техподдержки, в архив помещаются опасные и потенциально опасные файлы задания и все связанные с ними объекты.

При любом способе скачивания (кроме скачивания отдельного файла) в архив также помещаются файлы `registry.csv` и `metainfo.json` с информацией о файлах и результатах их проверки.

Оригинальное имя файла при скачивании заменяется на <Имя файла>.<Идентификатор объекта>.bin. Для каждого файла в архиве создается отдельная папка с названием <Имя файла>_<Идентификатор объекта>_(<Хеш-сумма SHA-256>).

Если для файла выполнялся поведенческий анализ, кроме самого файла в папку помещается отдельная папка с названием BA_<Название образа VM> для каждого образа VM, в котором проверялся файл. Такая папка содержит вложенные папки:

- `amsi` — с AMSI-скриптами;
- `dumps` — с файлами дампов памяти;
- `filesystem` — с dropped файлами;
- `logs` — с видеозаписью поведенческого анализа и дополнительными данными;
- `traces` — с результатами поведенческого анализа.

Скачивание отдельного файла

► Чтобы скачать отдельный файл:

1. В главном меню выберите **Объекты**.
2. Щелчком мыши по строке в таблице откройте карточку объекта.
3. В боковой панели в иерархическом списке выберите файл.
4. Нажмите кнопку **Скачать** и в раскрывшемся меню выберите **Выбранный файл**.

Примечание. Вы также можете скачать файл, наведя курсор на название файла в боковой панели и нажав ↓.

Файл добавлен в зашифрованный ZIP-архив с паролем `infected` и скачан на ваш компьютер.

Скачивание файлов задания

► Чтобы скачать файлы задания:

1. В главном меню выберите **Задания**.
2. Щелчком мыши по строке в таблице откройте карточку задания.
3. Если требуется скачать все файлы задания, в боковой панели нажмите кнопку **Скачать** и в раскрывшемся меню выберите **Все файлы**.
4. Если требуется скачать отфильтрованные файлы:
 - В боковой панели настройте фильтр файлов.
 - Нажмите кнопку **Скачать** и в раскрывшемся меню выберите **Отфильтрованные**.
5. Если требуется скачать один файл из задания:

- В боковой панели в иерархическом списке выберите нужный файл.
- Нажмите кнопку **Скачать** и в раскрывшемся меню выберите **Выбранный файл**.

Файлы задания добавлены в зашифрованный ZIP-архив с паролем `infected` и скачаны на ваш компьютер.

Скачивание информации о проверке для техподдержки

Если объект задания был неверно определен как опасный или потенциально опасный (ложное срабатывание), необходимо передать этот объект и информацию о его проверке в службу технической поддержки Positive Technologies для анализа.

Внимание! Для анализа ложных срабатываний средства проверки на основе машинного обучения PT ML необходимо собрать информацию как минимум о пяти схожих случаях ложного срабатывания. Такие случаи могут происходить в близкие промежутки времени, относиться к файлам одного типа и быть связаны с одной службой или приложением.

► Чтобы скачать информацию о проверке для техподдержки:

1. В главном меню выберите **Задания**.
2. Щелчком мыши по строке в таблице откройте карточку задания.
3. В боковой панели в иерархическом списке выберите:
 - Если требуется скачать информацию о проверке отдельного объекта, выберите этот объект.
 - Если требуется скачать информацию о проверке задания, выберите **Задание**.
4. В верхней части рабочей области страницы нажмите **i** → **Скачать файлы и результаты проверки**.

Примечание. Если необходимо, вы можете скачать только результаты проверки, нажав **i** → **Скачать результаты проверки**.

Информация о проверке и файлы задания добавлены в ZIP-архив с паролем `infected` и скачана на ваш компьютер.

5. Нажмите кнопку **Отчет по заданию** и сохраните отчет в формате PDF.

Полученные архив и отчет по заданию необходимо передать в службу технической поддержки Positive Technologies для анализа.

Файл registry.csv

Файл `registry.csv` содержит таблицу с информацией о скачанных файлах и результатах их проверки.

Таблица 3. Столбцы файла registry.csv

Столбец	Тип данных	Описание
node_id	Integer	Идентификатор объекта в задании
node_type	Enum	Тип элемента в карточке задания, который соответствует объекту: — ARTIFACT — карточка объекта; — SANDBOX — карточка поведенческого анализа; — SANDBOX_STAGE — карточка поведенческого анализа с перезагрузкой
object_type	Enum	Тип объекта задания: — ARCHIVE — архив; — COMPRESSED_FILE — сжатый файл; — EMAIL — письмо; — EMAIL_BODY — тело письма; — FILE — файл; — HTTP — HTTP-сообщение; — SANDBOX_AMSI — AMSI-скрипт; — SANDBOX_DROP — dropped файл; — SANDBOX_MEMORY_DUMP — дамп памяти (memdump); — SANDBOX_PROCESS_MEMORY_DUMP — дамп памяти (procdump); — URL — ссылка
mime	String	MIME-тип файла
is_threat	Boolean	Содержит ли объект угрозу
parent_id	Integer	Идентификатор родительского объекта в задании
name	String	Имя сохраненного файла или адрес ссылки
verdict	Enum	Тип обнаруженного вредоносного ПО (см. приложение Д.2)
path	String	Список идентификаторов всех родительских объектов в задании

Столбец	Тип данных	Описание
hash	String	Хеш-сумма SHA-256 объекта
properties	String	Метки объекта (см. приложение Г)
not_downloaded_reason	Enum	Причина, по которой файл не был скачан: — <code>ROTATED</code> — удален из хранилища файлов; — <code>NOT_A_FILE</code> — объект не является файлом
engine	String	Название средства проверки: — <code>antiphishing</code> — средство обнаружения угроз в почте PT Anti-Phishing and Anti-Spam; — <code>av.avast</code> — антивирус Avast Core Security; — <code>av.clamav</code> — антивирус ClamAV; — <code>av.kaspersky</code> — антивирус Kaspersky Web Traffic Security; — <code>av.ptav</code> — антивирус PT AV; — <code>av.vba</code> — антивирус VBA32; — <code>ptesc</code> — средство статического анализа на основе YARA-правил PT ESC; — <code>ptioc</code> — средство обнаружения индикаторов компрометации PT IoC; — <code>rule_engine</code> — дополнительные критерии определения потенциально опасных файлов; — <code>sandbox.network</code> — средство поведенческого анализа сетевых пакетов PT DPI; — <code>yara_engine</code> — средство проверки по пользовательским YARA-правилам (действующие правила); — <code>yara_engine_test</code> — средство проверки по пользовательским YARA-правилам (тестовые правила); — <code><Название образа VM></code> — образ VM, который использовался для поведенческого анализа

Столбец	Тип данных	Описание
engine_verdict	Enum	Тип обнаруженного средством проверки вредоносного ПО (см. приложение Д.2)
engine_version	String	Версия средства проверки
engine_db_version	String	Версия базы данных средства проверки
engine_detections	String	Название обнаруженной угрозы

11. Настройка средств проверки

Через интерфейс PT Email Security вы можете настраивать средства статического и динамического анализа объектов. В зависимости от средства проверки возможности по настройке различаются. Вы можете:

- Выбрать объекты, которые будут проверяться PT ESC.
- Указать домены, которым PT Categorizer не будет присваивать категории при обработке ссылок.
- Удалить или добавить базовые или пользовательские образы ВМ, которые будут доступны для динамического анализа объектов, настроить расписание обновления образов.
- Настроить время отображения файлов в очереди на поведенческий анализ и время повторного использования результатов поведенческого анализа.
- Добавить хеш-суммы файлов в черный или белый список или переместить их из одного списка в другой.
- Загрузить пакеты пользовательских YARA-правил, выполнить их отладку и перевести из тестовых в действующие.

В этом разделе

[Настройка средств проверки Positive Technologies \(см. раздел 11.1\)](#)

[Просмотр доступных антивирусов \(см. раздел 11.2\)](#)

[Настройка поведенческого анализа \(см. раздел 11.3\)](#)

[Работа с образами ВМ \(см. раздел 11.4\)](#)

[Работа с черным и белым списками \(см. раздел 11.5\)](#)

[Работа с пользовательскими YARA-правилами \(см. раздел 11.6\)](#)

11.1. Настройка средств проверки Positive Technologies

Для проверки объектов PT Email Security может использовать средства проверки, разработанные специалистами компании Positive Technologies. Для настройки таких средств проверки предназначена страница **Средства проверки** → **Экспертиза РТ**.

Статический анализ**PT ESC** Включен

Positive Technologies Expert Security Center

Версия 5.30.0.135310
Версия базы знаний 5.0.0.438 от 13 янв, 03:35
Проверяются Файлы, dropped файлы, дампы памяти, заголовки писем, AMSI-скрипты

[⚙ Параметры](#)**PT IoC** Включен

Positive Technologies Indicators of Compromise

Версия 5.30.0.135310
Версия базы знаний 1.1.0.843 от 12 янв, 23:37

Обработка ссылок**PT Crawler**

Positive Technologies Crawler

Версия 5.30.0.135310
Способ проверки ссылок Простой

PT Categorizer Включен

Positive Technologies Categorizer

Версия 5.30.0.135310
Версия базы знаний 1.0.0.1874 от 13 янв, 07:01

[⚙ Параметры](#)**Поведенческий анализ****PT ML** Включен

Positive Technologies Machine Learning

Версия 5.30.0.135310
Версия базы знаний 4.0.0.33 от 17 дек 2025, 08:23

PT DPI

Positive Technologies Deep Packet Inspection

Версия 12.3.7791
Версия сетевых правил 2.0.0.6164 от 13 янв, 14:14

Защита от угроз в почте**PT Anti-Phishing and Anti-Spam** Включен

Positive Technologies Anti-Phishing and Anti-Spam

Версия 5.30.0.135363
Версия базы знаний 1.0.0.43 от 17 дек 2025, 20:58

[⚙ Параметры](#)Рисунок 13. Страница **Экспертиза PT**

В рабочей области страницы расположены панели с информацией о средствах проверки, разделенные с помощью заголовков на группы:

- **Статический анализ** — средства проверки, использующие методы проверки, относящиеся к статическому анализу:
 - PT ESC — средство статического анализа на основе YARA-правил. По ссылке **Параметры** вы можете выбрать типы проверяемых объектов.
 - PT IoC — средство обнаружения индикаторов компрометации в файлах и ссылках.
- **Обработка ссылок** — средства проверки, предназначенные для работы со ссылками:
 - PT Crawler — средство динамической проверки ссылок.
 - PT Categorizer — средство категоризации ссылок. По ссылке **Параметры** вы можете указать имена доменов, исключаемых при категоризации ссылок. Ссылкам с такими доменами не будут присваиваться категории.
- **Поведенческий анализ** — средства проверки, использующие методы проверки, относящиеся к поведенческому анализу:
 - PT ML — средство поведенческого анализа на основе технологии машинного обучения.
 - PT DPI — средство поведенческого анализа сетевых пакетов.
- **Защита от угроз в почте** — средства проверки, предназначенные для проверки писем:
 - PT Anti-Phishing and Anti-Spam — средство проверки для выявления признаков фишинга и спама в письмах, а также для проверки найденных в письмах IP-адресов и имен доменов по спискам DNS-блокировок. По ссылке **Параметры** вы можете указать DNS-серверы для разрешения адресов.

Выбор объектов для проверки PT ESC

- ▶ Чтобы выбрать объекты для проверки PT ESC:
 1. В главном меню выберите **Средства проверки** → **Экспертиза РТ**.
 2. В панели с информацией о PT ESC перейдите по ссылке **Параметры**.
 3. В блоке параметров **Объекты для проверки** выберите объекты.
 4. Нажмите кнопку **Сохранить**.

Настройка категоризации ссылок

При проверке ссылок PT Email Security выполняет категоризацию ссылок и устанавливает для них соответствующие метки. Вы можете указать имена доменов, исключаемых при категоризации ссылок. Ссылкам с такими доменами не будут присваиваться категории.

► Чтобы указать имена доменов, исключаемых при категоризации ссылок:

1. В главном меню выберите **Средства проверки** → **Экспертиза РТ**.
2. В панели с информацией о PT Categorizer перейдите по ссылке **Параметры**.
3. В поле **Исключаемые домены** введите имя домена или поддомена и нажмите клавишу Enter.

Примечание. При вводе имен вы можете использовать звездочку в качестве подстановочного знака.

4. Если требуется указать другие имена, введите их аналогичным образом.
5. Нажмите кнопку **Сохранить**.

Выбор DNS-сервера для разрешения адресов

Разрешение адресов выполняется при их проверке по DNS-спискам блокировок. По умолчанию используется DNS-сервер кластера Kubernetes, развернутого в PT Email Security. Вы можете указать DNS-серверы вашей организации, которые будут использоваться для разрешения адресов.

► Чтобы ввести адрес DNS-сервера:

1. В главном меню выберите **Средства проверки** → **Экспертиза РТ**.
2. В панели с информацией о PT Anti-Phishing and Anti-Spam перейдите по ссылке **Параметры**.
3. Выберите вариант **Указать DNS-серверы**.
4. Введите доменное имя или IP-адрес DNS-сервера.
5. Нажмите кнопку **Сохранить**.

11.2. Просмотр доступных антивирусов

Кроме средств проверки, разработанных специалистами Positive Technologies, для проверки объектов в PT Email Security используются антивирусы сторонних разработчиков. Для просмотра доступных антивирусов предназначена страница **Средства проверки** → **Антивирусы**.

Основные

Антивирусы и их базы обновляются автоматически с серверов Positive Technologies.

ClamAV Включен

Cisco Talos

Последнее обновление базы 23 июня, 14:34

Версия 0.103.8 от 20 мая, 13:30

PT AV Включен

Positive Technologies

Последнее обновление базы 23 июня, 14:00

Версия 5.3490.0 от 17 июня, 11:21

VBA32 Отключен

«ВИРУСБЛОКАДА»

Дополнительные

Антивирусы нужно обновлять вручную. Их базы обновляются автоматически с серверов поставщиков.

Kaspersky Web Traffic Security Включен

«Лаборатория Касперского»

Последнее обновление базы 24 июня, 07:43

Версия продукта 6.1.0.4762

Версия ядра 6.1.0.4762

Установлен 24 июня, 09:44

Лицензия ✓ Действительна до 11 сентября

Рисунок 14. Страница **Антивирусы**

В рабочей области страницы расположены панели с информацией об антивирусах, разделенные с помощью заголовков на группы:

— **Основные** — входят в комплект поставки PT Email Security:

- ClamAV;
- PT AV;
- VBA32.

Базы и лицензии этих антивирусов обновляются автоматически.

— **Дополнительные** — добавлены в PT Email Security после его установки. Базы дополнительных антивирусов обновляются автоматически.

11.3. Настройка поведенческого анализа

Отправленные на поведенческий анализ файлы поступают на проверку в порядке очереди. Файлы в очереди сортируются по времени создания заданий на проверку и приоритету источника. Вы можете добавить в PT Email Security свои правила определения приоритетных

источников и задать приоритет проверки файлов от этих источников. Дополнительно можно добавить правила определения приоритетных типов файлов и установить приоритет для таких файлов. После настройки файлы в очереди будут сортироваться с учетом заданного приоритета источников и приоритета типов файлов.

Для удобства работы с очередью файлов на поведенческий анализ вы можете изменить время отображения проверенных файлов в очереди. Если на проверку в PT Email Security часто отправляются одинаковые файлы, вы можете изменить время повторного использования результатов поведенческого анализа.

Настройка правил определения приоритетных источников

Вы можете настроить правила определения приоритетных источников, файлы от которых необходимо отправлять на поведенческий анализ в первую очередь. Добавив несколько правил, вы сможете настроить приоритет источников. Дополнительно в каждом правиле вы можете указать приоритетные для выбранных источников типы и форматы файлов, а также метки файлов.

► Чтобы добавить правило определения приоритетных источников:

1. В главном меню выберите **Средства проверки** → **Поведенческий анализ** → **Приоритет файлов**.
2. В блоке параметров **Приоритет по источникам** нажмите кнопку **Добавить**.
3. В раскрывающемся списке **Источники** выберите источники, для которых необходимо изменить приоритет проверки файлов.
4. Если требуется, в раскрывающемся списке **Типы файлов** выберите типы и форматы файлов.
5. Если требуется, в раскрывающемся списке **Метки** выберите метки файлов.
6. Нажмите кнопку **Добавить**.
7. Нажмите кнопку **Сохранить**.

Правило будет добавлено в конец списка.

► Чтобы скопировать правило определения приоритетных источников:

1. В главном меню выберите **Средства проверки** → **Поведенческий анализ** → **Приоритет файлов**.
 2. В блоке параметров **Приоритет по источникам** в строке правила нажмите .
 3. Нажмите кнопку **Вставить правило**.
- Откроется окно **Добавление правила**.

4. Нажмите кнопку **Добавить**.

5. Нажмите кнопку **Сохранить**.

Правило будет добавлено в конец списка.

► Чтобы изменить правило определения приоритетных источников:

1. В главном меню выберите **Средства проверки** → **Поведенческий анализ** → **Приоритет файлов**.

2. В блоке параметров **Приоритет по источникам** в строке правила нажмите  .
Откроется окно **Изменение правила**.

3. Измените правило.

4. Нажмите кнопку **Изменить**.

5. Нажмите кнопку **Сохранить**.

► Чтобы удалить правило определения приоритетных источников:

1. В главном меню выберите **Средства проверки** → **Поведенческий анализ** → **Приоритет файлов**.

2. В блоке параметров **Приоритет по источникам** в строке правила нажмите  и подтвердите удаление.

3. Нажмите кнопку **Сохранить**.

Настройка приоритета источников

В списке **Приоритет по источникам** добавлены стандартные правила определения приоритетных источников, расположенные в порядке убывания приоритета источника. После добавления собственных правил для конкретных источников вы можете настроить их приоритет, расположив их в этом списке.

► Чтобы настроить приоритет источников:

1. В главном меню выберите **Средства проверки** → **Поведенческий анализ** → **Приоритет файлов**.

2. В блоке параметров **Приоритет по источникам** расположите строку добавленного вами правила согласно приоритету источника, используя  и  .

3. Нажмите кнопку **Сохранить**.

Настройка правил определения приоритетных типов файлов

Вы можете настроить правила определения приоритетных типов файлов, которые необходимо отправлять на поведенческий анализ в первую очередь. Добавив несколько правил, вы сможете настроить приоритет файлов в зависимости от их типов и форматов.

- ▶ Чтобы добавить правило определения приоритетных типов файлов:
 1. В главном меню выберите **Средства проверки** → **Поведенческий анализ** → **Приоритет файлов**.
 2. В блоке параметров **Приоритет по типам файлов** нажмите кнопку **Добавить**.
 3. В раскрывающемся списке **Типы файлов** выберите типы и форматы файлов.
 4. Если требуется, в раскрывающемся списке **Метки** выберите метки файлов.
 5. Нажмите кнопку **Добавить**.
 6. Нажмите кнопку **Сохранить**.

Правило будет добавлено в конец списка.

- ▶ Чтобы скопировать правило определения приоритетных типов файлов:
 1. В главном меню выберите **Средства проверки** → **Поведенческий анализ** → **Приоритет файлов**.
 2. В блоке параметров **Приоритет по типам файлов** в строке правила нажмите .
 3. Нажмите кнопку **Вставить правило**.
Откроется окно **Добавление правила**.
 4. Нажмите кнопку **Добавить**.
 5. Нажмите кнопку **Сохранить**.

Правило будет добавлено в конец списка.

- ▶ Чтобы изменить правило определения приоритетных типов файлов:
 1. В главном меню выберите **Средства проверки** → **Поведенческий анализ** → **Приоритет файлов**.
 2. В блоке параметров **Приоритет по типам файлов** в строке правила нажмите .
Откроется окно **Изменение правила**.
 3. Измените правило.
 4. Нажмите кнопку **Изменить**.
 5. Нажмите кнопку **Сохранить**.

- ▶ Чтобы удалить правило определения приоритетных типов файлов:
 1. В главном меню выберите **Средства проверки** → **Поведенческий анализ** → **Приоритет файлов**.
 2. В блоке параметров **Приоритет по типам файлов** в строке правила нажмите  и подтвердите удаление.
 3. Нажмите кнопку **Сохранить**.

Настройка приоритета типов файлов

По умолчанию файлы поступают на поведенческий анализ последовательно согласно времени создания задания на проверку и приоритету источника. После добавления правил определения приоритетных типов файлов вы можете настроить приоритет типов файлов, расположив правила в списке **Приоритет по типам файлов** в порядке убывания их приоритета.

- ▶ Чтобы настроить приоритет типов файлов:
 1. В главном меню выберите **Средства проверки** → **Поведенческий анализ** → **Приоритет файлов**.
 2. В блоке параметров **Приоритет по типам файлов** расположите строку добавленного вами правила согласно приоритету типов файлов, используя  и .
 3. Нажмите кнопку **Сохранить**.

Изменение времени отображения проверенных файлов в очереди

По умолчанию информация о проверенных файлах отображается в очереди в течение 5 дней.

- ▶ Чтобы изменить время отображения проверенных файлов в очереди на поведенческий анализ:
 1. В главном меню выберите **Средства проверки** → **Поведенческий анализ** → **Время хранения результатов**.
 2. В поле **Время отображения проверенных файлов в очереди** введите время в днях.
 3. Нажмите кнопку **Сохранить**.

Изменение времени повторного использования результатов

После завершения поведенческого анализа файла результат проверки некоторое время хранится в оперативной памяти сервера PT Email Security. Если такой же файл повторно поступает на поведенческий анализ в том же образе ВМ с такими же параметрами проверки, то вместо повторного анализа может быть использован результат предыдущей проверки из памяти сервера. Время повторного использования результатов должно быть меньше времени отображения проверенных файлов в очереди. По умолчанию это время составляет 48 часов.

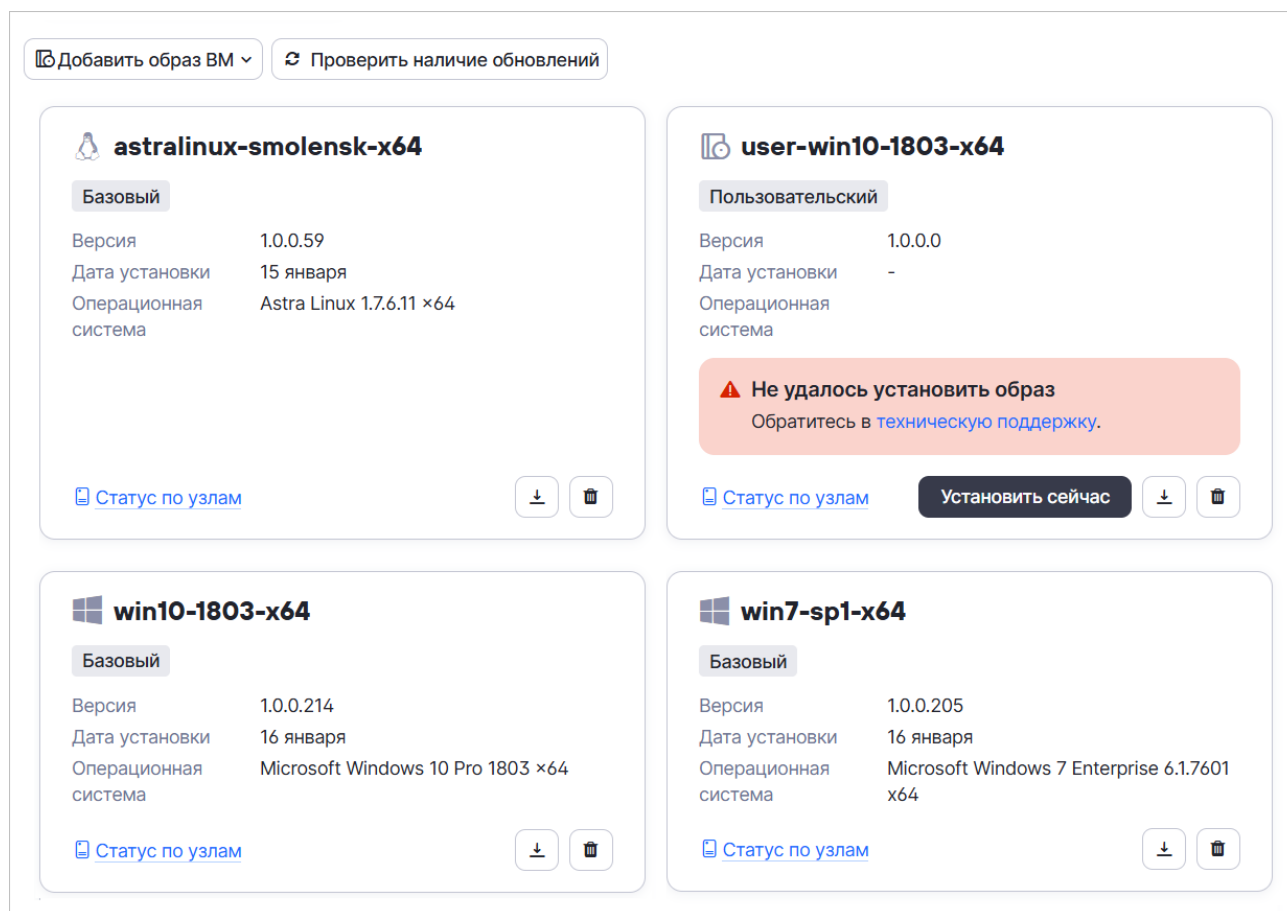
► Чтобы изменить время повторного использования результатов поведенческого анализа:

1. В главном меню выберите **Средства проверки** → **Поведенческий анализ** → **Время хранения результатов**.
2. В поле **Время повторного использования результатов** введите время в часах.
3. Нажмите кнопку **Сохранить**.

11.4. Работа с образами ВМ

Для проверки файлов методом поведенческого анализа PT Email Security использует различные образы виртуальных машин. Образы ВМ могут быть базовыми и пользовательскими. Специалисты Positive Technologies подготовили базовые образы ВМ популярных операционных систем, которые вы можете добавлять в PT Email Security через веб-интерфейс по мере необходимости. Дополнительно вы можете создавать пользовательские образы ВМ с помощью утилиты ImageBuilder и добавлять их в PT Email Security через веб-интерфейс. Любые образы можно скачивать и удалять.

Для работы с образами ВМ через веб-интерфейс предназначена страница **Средства проверки** → **Поведенческий анализ** → **Образы виртуальных машин** → **Управление образами**.

Рисунок 15. Страница **Образы VM**

В верхней части страницы расположены:

- Кнопка **Добавить образ VM** для добавления базовых или пользовательских образов VM.
- Кнопка **Проверить наличие обновлений** для ручной проверки наличия обновлений для образов VM на сервере Positive Technologies. Автоматическая проверка обновлений выполняется регулярно. При наличии новых версий образы автоматически скачиваются и устанавливаются.

В рабочей области страницы расположены панели с названиями установленных образов VM. Для каждого образа указаны: версия, дата установки и операционная система. В каждой панели также расположены:

- Метка типа образа:
 - **Базовый** — образ VM подготовлен специалистами Positive Technologies.
 - **Пользовательский** — пользовательский образ VM.

Внимание! Метка **ImageBuilder** указывает, что пользовательский образ VM был вручную скопирован на узлы PT Email Security с функцией поведенческого анализа. Рекомендуется с помощью утилиты ImageBuilder экспортировать этот образ в файл с расширением `.sandboximage` и повторно добавить его в PT Email Security через веб-

интерфейс. После этого необходимо заменить образ VM в параметрах проверки объектов от источников. Инструкцию по экспорту пользовательского образа VM вы можете найти в Руководстве разработчика PT Email Security.

- Ссылка **Статус по узлам** для просмотра информации об узлах, на которых установлен или устанавливается образ.
- Кнопка **Установить сейчас** для немедленного запуска установки образа. Кнопка отображается, если образ находится в очереди на установку.
- Кнопки  и  для скачивания и удаления образов.

Добавление базового образа VM

Перечень доступных вам базовых образов VM PT Email Security определяется вашей лицензией и указан на странице **Система** → **Лицензия**. Все образы VM из вашей лицензии автоматически устанавливаются в PT Email Security. При необходимости вы можете удалить образ и позже снова добавить его в PT Email Security.

Примечание. Если какой-либо образа VM из вашей лицензии недоступен для добавления в PT Email Security, обратитесь в техническую поддержку Positive Technologies.

► Чтобы добавить базовый образ VM:

1. В главном меню выберите **Средства проверки** → **Поведенческий анализ** → **Образы виртуальных машин** → **Управление образами**.
2. Нажмите кнопку **Добавить образ VM** → **Базовый**.
3. Отметьте флажками нужные образы и нажмите кнопку **Добавить**.

После окончания загрузки на странице **Образы VM** появится панель с названием образа.

Добавление пользовательского образа VM

Вы можете добавить образ VM только из файла с расширением `.sandboximage`, созданного с помощью утилиты ImageBuilder. Инструкции по созданию такого файла вы можете найти в Руководстве разработчика PT Email Security. Размер файла не должен превышать 30 ГБ.

Внимание! Для добавления образа необходимо обеспечить скорость передачи данных между рабочей станцией и основным узлом PT Email Security не менее 100 Мбит/с.

► Чтобы добавить пользовательский образ VM:

1. В главном меню выберите **Средства проверки** → **Поведенческий анализ** → **Образы виртуальных машин** → **Управление образами**.
2. Нажмите кнопку **Добавить образ VM** → **Пользовательский**.
3. В поле **Название образа** введите название.

Название должно содержать не меньше пяти символов. Используйте только латинские буквы, цифры, точку, дефис и символ подчеркивания.

4. По ссылке укажите расположение файла с образом.
5. Нажмите кнопку **Добавить**.

После окончания загрузки на странице **Образы ВМ** появится панель с названием образа.

Настройка расписания обновления образов ВМ

Вы можете указать интервалы времени, в которые новые образы будут скачиваться с сервера Positive Technologies и устанавливаться на узлы PT Email Security с функцией поведенческого анализа.

► Чтобы настроить расписание обновления образов ВМ:

1. В главном меню выберите **Средства проверки** → **Поведенческий анализ** → **Образы виртуальных машин** → **Режим обновления**.
2. В блоке параметров **Режим обновления** выберите режим скачивания и установки образов.
3. Если вы выбрали обновление по расписанию, настройте интервалы времени для обновления:
 - Нажмите кнопку **Добавить**.
 - Введите время начала и время окончания интервала.
 - Если требуется, добавьте еще интервал аналогичным образом.
4. Нажмите кнопку **Сохранить**.

Управление установкой образов ВМ

Установка образов ВМ на узлы PT Email Security с функцией поведенческого анализа может занимать продолжительное время. В очереди на установку образы сортируются по порядку их скачивания с сервера Positive Technologies. Вы можете управлять последовательностью установки образов, изменяя их положение в очереди.

► Чтобы настроить последовательность установки образов ВМ:

1. В главном меню выберите **Средства проверки** → **Поведенческий анализ** → **Образы виртуальных машин** → **Очередь обновления образов**.
2. Выберите образ ВМ.
3. Измените его положение в очереди:
 - Если необходимо переместить образ в начало очереди и запустить установку, нажмите кнопку **Установить сейчас**.

- Если необходимо переместить образ в начало очереди, нажмите кнопку **В начало очереди**.
 - Если необходимо переместить образ в очереди на одну позицию выше, нажмите кнопку **Выше**.
 - Если необходимо переместить образ в очереди на одну позицию ниже, нажмите кнопку **Ниже**.
 - Если необходимо переместить образ в конец очереди, нажмите кнопку **В конец очереди**.
4. Если требуется, измените положение других образов в очереди аналогичным образом.

Скачивание образа VM

► Чтобы скачать образ VM:

1. В главном меню выберите **Средства проверки** → **Поведенческий анализ** → **Образы виртуальных машин** → **Управление образами**.
2. В панели с информацией об образе VM нажмите .

Удаление образа VM

► Чтобы удалить образ VM:

1. В главном меню выберите **Средства проверки** → **Поведенческий анализ** → **Образы виртуальных машин** → **Управление образами**.
2. В панели с информацией об образе VM нажмите  и подтвердите удаление.

Внимание! Если образ VM используется какими-либо источниками, в окне подтверждения будут указаны названия этих источников. При необходимости в параметрах проверки указанных источников вы можете выбрать другой образ VM для поведенческого анализа файлов.

11.5. Работа с черным и белым списками

Проверка хеш-сумм файла по черному и белому спискам в PT Email Security является одним из методов проверки объектов и учитывается при вынесении вердикта.

Обнаружение файла в черном списке является достаточным условием для вынесения вердикта об опасности файла. В этот список вы можете добавить файлы, которые представляют угрозу, но при проверке были ошибочно признаны безопасными. При обнаружении файла в белом списке выносится вердикт о безопасности файла. В этот список вы можете добавить файлы, в безопасности которых вы уверены, но которые были ошибочно признаны опасными, например, из-за ложного срабатывания антивируса.

Примечание. При проверке файлов через веб-интерфейс вы можете указать, нужно ли продолжать проверку файла после его обнаружения в черном или белом списке.

Если у вас есть хеш-суммы заведомо опасных или безопасных файлов, полученные из внешних источников, например из экспертного центра или из другого экземпляра PT Email Security, вы можете импортировать их в черный или белый список. Кроме того, после проверки любого файла вы можете добавить его в черный или белый список из карточки объекта. По результатам повторной проверки файла или после получения новой информации о файле из внешних источников вы можете перенести его хеш-сумму из одного списка в другой.

Для работы с хеш-суммами файлов, которые добавлены в черный и белый списки предназначены **Средства проверки** → **Черный список** и **Средства проверки** → **Белый список**. Страницы имеют схожий вид, на каждой из страниц вы можете просматривать хеш-суммы, добавлять и удалять их из списков. Вы также можете переносить хеш-суммы из одного списка в другой.

Добавить хеш-суммы		Скачать список			
Переместить в белый список Удалить из списка Очистить					
☐	Дата добавления За все время	Тип хеш-суммы	Хеш-сумма	Кто добавил	Комментарий
☐	14 фев, 16:14	SHA-256	8063899592bbfe5faebcd1aeb726ec665efdb...	Ivanov	
☐	14 фев, 16:14	SHA-256	d4d33cba6bfca07034567b1bb13baac34c67...	Ivanov	
☐	14 фев, 16:12	MD5	6054aa83a6313692076b5622a4a75d94	Ivanov	Срочно проверить
☐	14 фев, 16:12	SHA-256	64615acc0ec25aff9cdc1f20e428a90861300...	Ivanov	Подозрительный файл
☐	14 фев, 16:11	SHA-256	13d17df7126ab5a1d163868ef14f5d27cf8aa8...	Ivanov	
☐	14 фев, 16:10	SHA-256	d79727e2b98b6a771a57559f756e6c3bf641e...	Administrator	
☐	14 фев, 16:09	MD5	dffcb9e0cba98ddcf6716b7b308adc4d	Administrator	
Всего 15				1 < >	

Рисунок 16. Страница **Черный список**

В панели инструментов каждой страницы расположены кнопки для работы со списком хеш-сумм:

- **Добавить хеш-суммы** — для добавления хеш-сумм в список вручную или из CSV-файла.
- **Скачать список** — для экспорта списка хеш-сумм в CSV-файл.

Ниже расположены кнопки для работы с хеш-суммами в списке:

- **Переместить в белый список** или **Переместить в черный список** — для переноса выбранных хеш-сумм из одного списка в другой.

Примечание. Для выбора в таблице нескольких хеш-сумм вы можете установить для них флажки в первом столбце, для выбора всех хеш-сумм — установить флажок в заголовке первого столбца.

- **Удалить из списка** — для удаления выбранных хеш-сумм.
- **Очистить** — для удаления всех хеш-сумм из списка.

В таблице отображаются столбцы с информацией о добавленных в список хеш-суммах:

- **Дата добавления** — дата добавления в список. Нажав на заголовок столбца, вы можете настроить фильтр по времени добавления хеш-суммы в список.
- **Тип хеш-суммы** — тип SHA-256, SHA-1 или MD5. Нажав на заголовок столбца, вы можете настроить фильтр по типам хеш-сумм.
- **Хеш-сумма** — хеш-сумма. При нажатии на заголовок столбца появляется поле для поиска хеш-суммы.
- **Кто добавил** — логин пользователя, который добавил хеш-сумму в список. При нажатии на заголовок столбца появляется поле для поиска логина.
- **Комментарий** — любой текстовый комментарий. При нажатии на заголовок столбца появляется поле для поиска комментария.

Примечание. При наведении курсора на строку таблицы в ней появляются кнопки для работы с отдельными хеш-суммами. По кнопке  вы можете изменить комментарий, по кнопке  — скопировать хеш-сумму, по кнопке  — перенести хеш-сумму из одного списка в другой, по кнопке  — удалить.

Добавление хеш-сумм в черный или белый список

- Чтобы добавить хеш-суммы файлов в черный (белый) список:

1. В главном меню выберите **Средства проверки** → **Черный список (Белый список)**.
2. Нажмите кнопку **Добавить хеш-суммы**.
3. Если вы хотите ввести хеш-суммы вручную, введите их в поле **Хеш-суммы**.

Несколько хеш-сумм вы можете ввести в отдельных строках или в одной строке, используя в качестве разделителя пробел, запятую, табуляцию, точку с запятой или вертикальную черту.

4. Если вы хотите импортировать хеш-суммы из файла, нажмите кнопку **Выберите файл** и укажите его расположение.

Импортировать хеш-суммы вы можете из CSV-файла с кодировкой UTF-8. Хеш-суммы будут импортированы только из первого столбца файла.

5. Нажмите кнопку **Добавить**.

Перемещение хеш-сумм между списками

- ▶ Чтобы переместить хеш-суммы из одного списка в другой:
 1. В главном меню выберите **Средства проверки** → **Черный список (Белый список)**.
 2. Выберите хеш-суммы в таблице.
 3. В панели инструментов нажмите кнопку **Переместить в белый список (Переместить в черный список)**.

Удаление хеш-сумм из черного или белого списка

- ▶ Чтобы удалить хеш-суммы из черного (белого) списка:
 1. В главном меню выберите **Средства проверки** → **Черный список (Белый список)**.
 2. Выберите хеш-суммы в таблице.
 3. В панели инструментов нажмите кнопку **Удалить из списка** и подтвердите удаление.

Очистка черного или белого списка

- ▶ Чтобы удалить хеш-суммы из черного (белого) списка:
 1. В главном меню выберите **Средства проверки** → **Черный список (Белый список)**.
 2. В панели инструментов нажмите кнопку **Очистить** и подтвердите удаление всех хеш-сумм.

11.6. Работа с пользовательскими YARA-правилами

Для проверки объектов в PT Email Security вы можете использовать созданные вами YARA-правила. Для работы с такими правилами используется средство проверки по пользовательским YARA-правилам.

Для работы с пользовательскими YARA-правилами предназначена страница **Средства проверки** → **Пользовательские правила**.

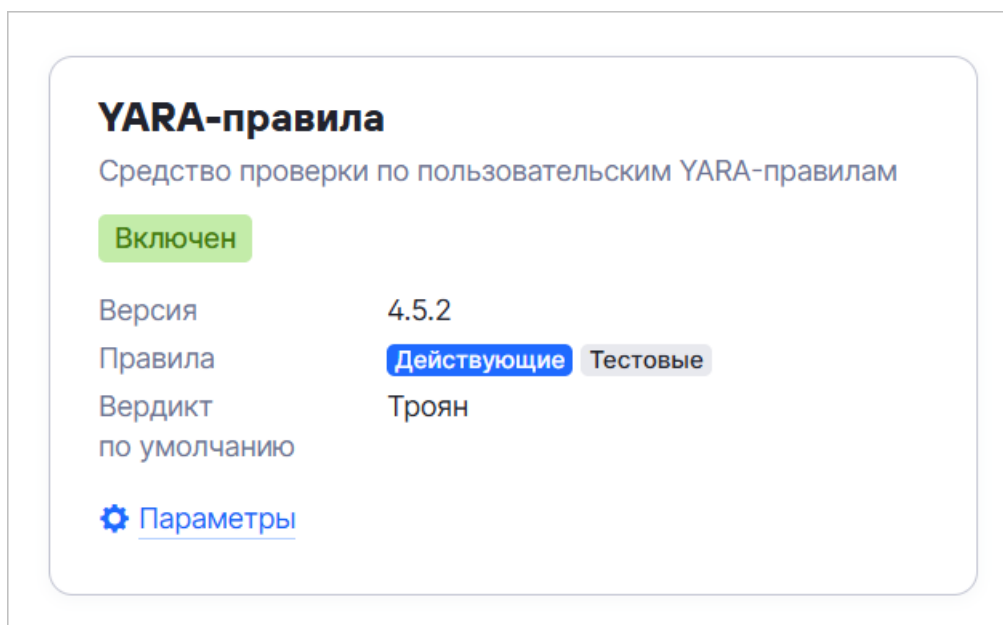


Рисунок 17. Страница **Пользовательские правила**

В рабочей области страницы расположена панель с информацией о средстве проверки по пользовательским YARA-правилам. В панели отображаются:

- Статус средства проверки. Если средство проверки отключено, вы не можете работать с YARA-правилам.
- Версия средства проверки.
- Статус добавленных правил: **Действующие** — результат проверки по таким правилам учитывается при вынесении вердикта; **Тестовые** — результат проверки отображается в карточке объекта, но не влияет на вердикт.
- Ссылка **Параметры** для работы с YARA-правилами.

Работа с YARA-правилами

Подробную информацию по созданию YARA-правил вы можете получить [на сайте документации YARA](#).

Для использования разработанных вами YARA-правил в PT Email Security вам необходимо:

1. Подготовить правила для работы в PT Email Security. Для каждого правила в блоке `meta` вы можете указать информацию о вредоносном ПО, которое обнаруживает правило.
 - Если требуется указать тип вредоносного ПО, можно добавить параметр `malware_class`. Значение этого параметра будет указано в вердикте по объекту и должно соответствовать [типам вредоносного ПО, используемым в QL-запросах](#) (см. приложение Д.2).

Примечание. Если тип вредоносного ПО не указан в YARA-правиле, то для объекта будет вынесен вердикт по умолчанию, выбранный в параметрах средства проверки по пользовательским YARA-правилам.

- Если требуется указать класс и операционную систему вредоносного ПО, можно добавить параметры `malware_family` и `platform`. В качестве класса вы можете указать любой текст, в качестве операционной системы одно из значений: `ANDROID`, `IOS`, `LINUX`, `NO_PLATFORM`, `OSX`, `WINDOWS`.
2. Сформировать пакет правил, объединив в один текстовый файл все правила, которые вы планируете использовать для проверки объектов.
 3. Добавить пакет правил в PT Email Security в качестве тестовых YARA-правил. Результат проверки по таким правилам отображается в карточке объекта, но не учитывается при вынесении вердикта.
 4. Провести проверку YARA-правил на ложные срабатывания и их отладку. В процессе отладки вы можете заменять один пакет тестовых правил другим, при этом автоматически будет обновляться версия пакета.
 5. Перевести тестовые YARA-правила в действующие. Результат проверки по таким правилам учитывается при вынесении вердикта по объекту.

Результат проверки объектов по пользовательским YARA-правилам вы можете находить с помощью QL-запросов. Например, для поиска по указанным вами в правилах значениям параметров `malware_class`, `malware_family` и `platform` вы можете использовать поля:

- Для тестовых правил — `yara_engine_test.detections.threat.classification`, `yara_engine_test.detections.threat.family`, `yara_engine_test.detections.threat.platform`;
- Для действующих правил — `yara_engine.detections.threat.classification`, `yara_engine.detections.threat.family`, `yara_engine.detections.threat.platform`.

Пример YARA-правил:

```
rule tool_win_ZZ_OfficeMacro_Risktool_OOXMLMacroSheet_Artifact
{
  meta:
    malware_class = "RISKTOOL"
    malware_family = "OfficeMacro"
    platform = "WINDOWS"
  strings:
    $TFBM =
"\x20\x54\x61\x72\x67\x65\x74\x3d\x22\x6d\x61\x63\x72\x6f\x73\x68\x65\x65\x74"
    $fwNs = "\x3c\x78\x6d\x3a\x6d\x61\x63\x72\x6f\x73\x68\x65\x65\x74\x20"
  condition:
    any of them
}
```

Добавление тестовых YARA-правил

► Чтобы добавить YARA-правила:

1. В главном меню выберите **Средства проверки** → **Пользовательские правила**.
2. В панели **YARA-правила** перейдите по ссылке **Параметры**.
3. Нажмите кнопку **Загрузить**.
4. Перетащите файл с пакетом YARA-правил в область загрузки и нажмите кнопку **Загрузить**.

Поддерживаются только текстовые файлы.

5. В раскрывающемся списке **Вердикт по умолчанию** выберите вердикт, который будет выноситься по правилам без вердикта.
6. Нажмите кнопку **Сохранить**.

Перевод тестовых YARA-правил в действующие

► Чтобы перевести тестовые YARA-правила в действующие:

1. В главном меню выберите **Средства проверки** → **Пользовательские правила**.
2. В панели **YARA-правила** перейдите по ссылке **Параметры**.
3. Нажмите кнопку **Перевести в действующие**.
4. Нажмите кнопку **Сохранить**.

Замена пакета тестовых YARA-правил

► Чтобы заменить пакет тестовых YARA-правил:

1. В главном меню выберите **Средства проверки** → **Пользовательские правила**.
2. В панели **YARA-правила** перейдите по ссылке **Параметры**.
3. В строке тестовых правил нажмите ⇄.
4. Перетащите файл с пакетом YARA-правил в область загрузки и нажмите кнопку **Загрузить**.
5. Нажмите кнопку **Сохранить**.

Скачивание пакета YARA-правил

► Чтобы скачать пакет YARA-правил:

1. В главном меню выберите **Средства проверки** → **Пользовательские правила**.
2. В панели **YARA-правила** перейдите по ссылке **Параметры**.
3. В строке правила нажмите .
4. Нажмите кнопку **Сохранить**.

Удаление пакета YARA-правил

► Чтобы удалить пакет YARA-правил:

1. В главном меню выберите **Средства проверки** → **Пользовательские правила**.
2. В панели **YARA-правила** перейдите по ссылке **Параметры**.
3. В строке правила нажмите  и подтвердите удаление.
4. Нажмите кнопку **Сохранить**.

12. Настройка основных параметров PT Email Security

Для настройки основных параметров PT Email Security предназначена страница **Основные параметры**. Страница открывается при выборе в главном меню **Система** → **Основные параметры**.

Повторная проверка

Первая проверка выполняется при попадании файлов в систему. Файлы, пропущенные в инфраструктуру, можно проверить повторно после обновления баз.

Интервалы между первой и повторными проверками

Вы можете указать до пяти интервалов для повторных проверок. Отсчет каждого интервала начинается с момента первой проверки.

Первый интервал

1

день

+ Добавить интервал

Стандартные пароли

Для проверки содержимого архивов, защищенных паролем, PT Sandbox пытается распаковывать их используя стандартные пароли.

Пароли

infected

Введите по одному паролю в каждой строке. Чем больше паролей, тем дольше может выполняться распаковка архива, защищенного паролем

Сохранить

Отмена

Рисунок 18. Страница **Основные параметры**

В рабочей области страницы расположены следующие блоки параметров:

- **Повторная проверка** — для настройки повторной проверки файлов из хранилища.
- **Стандартные пароли** — для ввода паролей, которые будут использоваться при распаковке архивов.

В нижней части страницы расположены кнопки **Сохранить** и **Отменить** для применения или отмены внесенных изменений.

Настройка повторной проверки файлов

Файлы всех заданий после проверки сохраняются в хранилище. Вы можете настроить до пяти повторных проверок файлов в хранилище. Использование при каждой повторной проверке обновленных антивирусных баз и баз знаний средств проверки Positive Technologies позволяет обнаруживать опасные и потенциально опасные файлы, которые раньше считались безопасными.

Поведенческий анализ при повторной проверке не выполняется.

► Чтобы настроить повторную проверку файлов:

1. В главном меню выберите **Система** → **Основные параметры**.
2. В блоке параметров **Повторная проверка** включите повторную проверку.
3. В поле **Первый интервал** введите количество дней с момента сохранения файла в хранилище до запуска первой повторной проверки.
4. Если необходима еще одна повторная проверка, нажмите кнопку **Добавить интервал** и введите количество дней с момента сохранения файла в хранилище до запуска второй повторной проверки.

Примечание. Вы можете добавить до четырех дополнительных интервалов. Каждый интервал отсчитывается с момента сохранения файла в хранилище должен быть больше предыдущего.

5. Нажмите кнопку **Сохранить**.

Настройка списка стандартных паролей

Внимание! Большой список стандартных паролей может значительно увеличить время проверки зашифрованных архивов.

Для проверки зашифрованного архива PT Email Security пытается распаковать его, последовательно перебирая пароли, пока не будет найден подходящий. Сперва проверяются все пароли, которые были указаны в параметрах проверки, а затем стандартные пароли. Если подобрать пароль не удастся, содержимое архива не проверяется.

► Чтобы настроить список стандартных паролей:

1. В главном меню выберите **Система** → **Основные параметры**.
2. В блоке параметров **Стандартные пароли** в поле **Пароли** введите по одному паролю в каждой строке.
3. Нажмите кнопку **Сохранить**.

Список стандартных паролей будет применен через несколько минут.

13. Просмотр токенов доступа

Токен доступа — это уникальная последовательность символов, которая применяется для защиты PT Email Security от несанкционированного доступа через публичный API.

Все токены, созданные для доступа к PT Email Security по API, отображаются в веб-интерфейсе на странице **Система** → **Токены доступа**.

↶ Вернуться к фильтру по умолчанию

Дата создания За все время	Кто создал	Название	Связанный источник	Разрешенные действия	Комментарий
27 апр 2024, 13:49	Administrator	token-edr	edr-emakridi	Проверка с параметрами источника	
17 апр 2024, 16:59	Administrator	test		Проверка с передаваемыми параметрами, ...	
22 мар 2024, 15:32	Administrator	maxpatroledr		Проверка с параметрами источника	
14 мар 2024, 13:20	Administrator	maxpatroledrtoken		Проверка с параметрами источника	
6 мар 2024, 09:59	Administrator	oc-token	oc-entrpoint	Проверка с параметрами источника	
6 мар 2024, 09:34	Administrator	oc-key		Проверка с передаваемыми параметрами	
21 фев 2024, 15:06	Administrator	api-entry-point-token	api-entry-point	Проверка с параметрами источника	
26 янв 2024, 05:06	Administrator	ptcs2avscanner	ptcs-av-scanner	Проверка с передаваемыми параметрами, ...	for PT CS

Всего 70

1 2 < >

Рисунок 19. Страница **Токены доступа**

В рабочей области страницы расположена таблица с информацией по всем созданным токенам доступа. Вы можете перейти к источнику, для которого используется токен доступа, нажав на ссылку в столбце **Связанный источник**.

14. Работа с источниками

Источник для проверки (источник) — интерфейс в информационной системе организации, с которого в PT Email Security поступают объекты на проверку.

Объекты могут поступать на проверку от встроенных источников, которые не требуется добавлять в PT Email Security, и от подключаемых внешних источников, которые необходимо добавлять в PT Email Security в соответствии с их типами.

Встроенные источники

В PT Email Security предусмотрены следующие встроенные источники:

- Веб-интерфейс — вы можете анонимно или после входа в PT Email Security отправить объекты на проверку через веб-интерфейс. Поддерживается проверка объектов размером до 1 ГБ.
- Хранилище файлов — после настройки параметров повторной проверки PT Email Security регулярно проверяет файлы в хранилище.
- API с передаваемыми параметрами проверки — внешняя система может передавать объекты на проверку через службу публичного API PT Email Security. Проверка выполняется с параметрами, переданными в запросе. Поддерживается проверка объектов размером до 1 ГБ.

Подключаемые источники

Источником объектов для PT Email Security может служить внешняя система, например почтовый сервер, межсетевой экран или папки на сетевом диске. При подключении внешней системы, как правило, требуется настроить саму систему для работы с PT Email Security и добавить эту систему в PT Email Security в качестве источника. Для подключения различных типов внешних систем предусмотрены следующие типы источников:

- Служба Checkme — служба для проверки объектов по электронной почте, обеспечивает взаимодействие PT Email Security с почтовым сервером вашей организации. После настройки этого источника для проверки объекта достаточно отправить его письмом на специальный адрес электронной почты. PT Email Security проверит само письмо, ссылки в тексте письма и вложенные в него файлы. Результат проверки отправляется в ответном письме. Поддерживается проверка писем размером до 1 ГБ.
- Общая папка — папка с настроенным общим доступом, все файлы которой проверяются PT Email Security. После проверки все файлы остаются в той же папке. Поддерживается проверка файлов размером до 5 ГБ.
- Папка-шлюз — папка с настроенным общим доступом, все файлы которой проверяются PT Email Security. По результатам проверки объекты из папки-шлюза переносятся в папку для безопасных объектов или папку карантина. Поддерживается проверка файлов размером до 5 ГБ.

- ICAP-сервер — позволяет принимать на проверку объекты по протоколу ICAP. Для этого в PT Email Security настраивается ICAP-сервер, а внешняя система выступает в качестве ICAP-клиента. Поддерживается проверка объектов размером до 1 ГБ.
- Почтовый шлюз безопасности — позволяет получать письма от SMTP-сервера, развернутого на внешнем узле. Такой сервер принимает письма от SMTP-клиентов и работает в качестве почтового шлюза.
- Сервер Microsoft Exchange с установленным агентом — позволяет принимать почтовый трафик сервера Microsoft Exchange, перенаправляемый с помощью почтового агента PT Email Security. Почтовый агент устанавливается на сервер Microsoft Exchange, перехватывает все проходящие через сервер письма и отправляет их на проверку в PT Email Security, после чего возвращает проверенные письма обратно для доставки адресатам. Поддерживается проверка писем размером до 1 ГБ.
- Почтовый сервер в режиме фильтрации — позволяет принимать от почтового сервера, работающего в режиме фильтрации, письма для проверки в PT Email Security. Поддерживается проверка писем размером до 1 ГБ.

Режим фильтрации — режим работы почтового сервера, при котором PT Email Security может фильтровать почтовый трафик сервера. В зависимости от выбранного режима проверки PT Email Security либо сразу возвращает почтовому серверу отправленное на проверку письмо (пассивный режим), либо блокирует его до окончания проверки (блокирующий режим).

- Почтовый сервер в режиме фильтрации (MTA) — позволяет то же что и почтовый сервер в режиме фильтрации, но для работы с письмами используется встроенный в PT Email Security почтовый транспортный агент. Поддерживается проверка писем размером до 1 ГБ.
- Почтовый сервер в режиме зеркалирования — позволяет принимать от почтового сервера, работающего в режиме зеркалирования, скрытые копии писем для проверки в PT Email Security. Поддерживается проверка писем размером до 1 ГБ.

Режим зеркалирования — режим работы почтового сервера, при котором PT Email Security не влияет на почтовый трафик сервера. На проверку в PT Email Security отправляются копии писем.

- PT NAD — позволяет настроить интеграцию с PT NAD. После интеграции извлеченные из сетевого трафика файлы отправляются на проверку в PT Email Security. Поддерживается проверка файлов размером до 1 ГБ.
- MaxPatrol EDR — позволяет настроить интеграцию с MaxPatrol EDR. После интеграции извлеченные файлы конечных устройств отправляются на проверку в PT Email Security. Поддерживается проверка файлов размером до 1 ГБ.
- API с выбранными параметрами проверки — позволяет настроить интеграцию с внешними системами через сервис публичного API PT Email Security. Поддерживается проверка объектов размером до 1 ГБ.

Параметры проверки объектов, поступающих от источника, настраиваются индивидуально для каждого источника после его добавления в PT Email Security. Параметры проверки могут отличаться для источников разных типов.

Режимы проверки объектов, поступающих от источников

В зависимости от способа обработки объектов, поступающих на проверку в PT Email Security, предусмотрены следующие режимы проверки:

- Режим ожидания — режим проверки, при котором на проверку от источников в PT Email Security поступают копии объектов, а их распространение контролирует пользователь или сторонняя система.
- Пассивный режим — режим проверки, при котором поступившие на проверку объекты сразу пропускаются PT Email Security в информационную систему.
- Блокирующий режим — режим проверки, при котором поступившие на проверку объекты блокируются PT Email Security до окончания проверки. В зависимости от вынесенного вердикта объект пропускается в информационную систему или удаляется (или помещается в карантин).

Примечание. Использование блокирующего режима может быть ограничено лицензией.

Режимы проверки для каждого типа источника указаны в таблице. Для источников, поддерживающих несколько режимов проверки, выбор режима зависит от политики информационной безопасности вашей организации. Вы можете настроить режим проверки объектов для таких источников в параметрах проверки. Для источников с типом «ICAP-сервер» режим проверки настраивается в параметрах ICAP-клиента.

Таблица 4. Режимы проверки объектов, поступающих от источников

Тип источника	Режим ожидания	Пассивный режим	Блокирующий режим
Веб-интерфейс	Да	—	—
Хранилище файлов	Да	—	—
Служба Checkme	Да	—	—
Общая папка	—	Да	—
Папка-шлюз	—	Да	Да
ICAP-сервер	Да	Да	Да
Почтовый шлюз безопасности	—	Да	Да
Сервер Microsoft Exchange с установленным агентом	—	Да	Да
Почтовый сервер в режиме фильтрации	—	Да	Да
Почтовый сервер в режиме фильтрации (MTA)	—	Да	Да
Почтовый сервер в режиме зеркалирования	—	Да	—

Тип источника	Режим ожидания	Пассивный режим	Блокирующий режим
PT NAD	—	Да	—
MaxPatrol EDR	Да	—	—
API с выбранными параметрами проверки	Да	—	—
API с передаваемыми параметрами проверки	Да	—	—

В этом разделе

[Настройка параметров проверки объектов от источников \(см. раздел 14.1\)](#)

[Параметры проверки объектов от источников \(см. раздел 14.2\)](#)

[Настройка правил приема писем для почтового шлюза безопасности \(см. раздел 14.3\)](#)

[Настройка обработки писем по правилам \(см. раздел 14.4\)](#)

[Настройка блокирующего режима проверки писем \(см. раздел 14.5\)](#)

[Настройка блокирующего режима проверки файлов \(см. раздел 14.6\)](#)

[Настройка пользовательских правил определения файлов с угрозами \(см. раздел 14.7\)](#)

[Настройка проверки архивов \(см. раздел 14.8\)](#)

[Настройка проверки ссылок \(см. раздел 14.9\)](#)

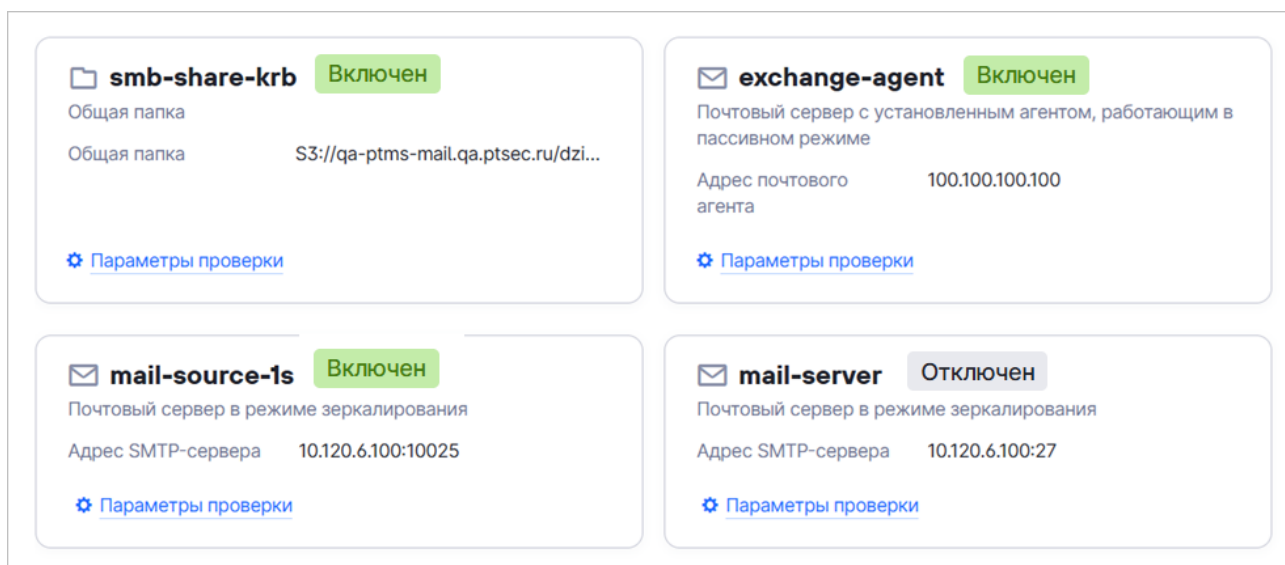
[Настройка пользовательских правил определения ссылок с угрозами \(см. раздел 14.10\)](#)

[Отключение сохранения файлов без угроз в хранилище \(см. раздел 14.11\)](#)

[Настройка правил поведенческого анализа \(см. раздел 14.12\)](#)

14.1. Настройка параметров проверки объектов от источников

PT Email Security может проверять объекты, поступающие от пользователей или из внешних систем, подключенных в качестве источников объектов. Для просмотра информации о подключенных источниках и настройки параметров проверки поступающих от них объектов предназначена страница **Источники**. Страница открывается при выборе в главном меню раздела **Источники**.

Рисунок 20. Страница **Источники**

В рабочей области страницы расположены панели с информацией о добавленных источниках. В каждой панели расположена ссылка **Параметры проверки** для настройки параметров проверки объектов, поступающих с источника.

Настройка параметров проверки объектов

- ▶ Чтобы настроить параметры проверки объектов от источника:
 1. В главном меню выберите **Источники**.
 2. В панели с информацией об источнике перейдите по ссылке **Параметры проверки**.
 3. Настройте [параметры проверки объектов от источника](#) (см. раздел 14.2).
 4. Нажмите кнопку **Сохранить**.

Просмотр заданий источника

- ▶ Чтобы просмотреть задания, отправленные с источника:
 1. В главном меню выберите **Источники**.
 2. Нажмите на панель источника.
 3. Выберите вкладку **Задания**.

На вкладке отображаются сведения о заданиях, отправленных с этого источника. Вы также можете настраивать столбцы, фильтровать и сортировать по ним задания.

14.2. Параметры проверки объектов от источников

Вы можете настраивать параметры проверки объектов, поступающих от источника, нажав в блоке с информацией об источнике кнопку **Параметры проверки**. Параметры проверки сгруппированы в следующие блоки.

Примечание. Если используются правила обработки писем, недоступны выбор режима проверки и некоторые параметры проверки (исключения, обезвреживание писем, карантин и блокировка подозрительных файлов).

Режим проверки

Выбор режима проверки поддерживается для источников «Почтовый сервер в режиме фильтрации», «Сервер Microsoft Exchange с установленным агентом» и «Папка-шлюз»². Доступны следующие режимы проверки писем (файлов) от источников:

- **Пассивный** — письма доставляются адресатам до завершения проверки.
- **Блокирующий** — письма задерживаются на почтовом сервере до получения результатов проверки.

Примечание. Выбор блокирующего режима проверки возможен, если приобретенная лицензия позволяет блокировать распространение писем и почтовый сервер организации поддерживает этот режим. В остальных случаях используется пассивный режим.

Для источника, работающего в блокирующем режиме, в блоке параметров **Пропускать письма в информационную систему** вы можете выбрать, когда нужно пропускать письма в информационную систему:

- **После завершения динамического анализа** — письма пропускаются после завершения поведенческого анализа файлов и проверки контента по ссылкам. Если динамический анализ не будет завершен в течение времени ожидания результатов проверки, письмо пропускается в информационную систему.

Примечание. Для динамического анализа писем в блокирующем режиме проверки необходимо, чтобы тайм-аут SMTP-сессии на почтовом сервере превышал максимальное время ожидания результатов проверки в PT Email Security. Если в течение SMTP-сессии письмо не будет проверено или нарушится связь почтового сервера с PT Email Security, письмо будет повторно отправлено на проверку и в PT Email Security для него будет создано новое задание.

- **Не дожидаясь завершения динамического анализа** — если статический анализ не обнаружил угроз, письма пропускаются в информационную систему сразу после его завершения.

² Для источника «ICAP-сервер» выбор и настройка режимов проверки выполняются на ICAP-клиенте. При проверке файлов от этого источника доступны блокирующий и пассивный режимы, а также режим ожидания.

Максимальное время ожидания результатов проверки — для источника, работающего в блокирующем режиме, в этом поле необходимо указать максимальное время, на которое будут задерживаться письма. По истечении этого времени письма пропускаются в информационную систему до получения результатов проверки.

Внимание! При включенном поведенческом анализе файлов максимальное время ожидания результатов проверки должно быть больше продолжительности наблюдения за файлом в каждом из выбранных образов. В противном случае проверяемые в этих образах файлы будут пропускаться в информационную систему до получения результатов поведенческого анализа.

Вид страницы с уведомлением о блокировке

Если при проверке ссылки обнаружен вредоносный контент, доступ по ссылке блокируется, а пользователю вместо исходной страницы отображается страница с уведомлением о блокировке. Для источника «ICAP-сервер» можно настроить вид этой страницы.

В блоке параметров **Показывать на странице** вы можете выбрать какая информация будет отображаться на странице с уведомлением о блокировке:

- **Тип вредоносного ПО** — тип обнаруженного по ссылке [вредоносного ПО](#) (см. приложение Д.2).
- **Идентификатор задания** — идентификатор задания на проверку ссылки.
- **Сообщение** — позволяет добавить произвольное сообщение.

Максимальное время выполнения задания

В этом поле вы можете указать время в секундах, по истечении которого задание будет принудительно завершено без вынесения вердикта. Это время должно быть больше или равно времени, указанного в поле **Максимальное время ожидания результатов проверки**.

Исключения

Для источника, работающего в блокирующем режиме, в этом блоке в поле **Эл. адреса получателей** вы можете указать адреса электронной почты, письма на которые не будут блокироваться, независимо от результата проверки.

Обезвреживание писем

Для источника, работающего в блокирующем режиме, вы можете настроить обезвреживание всех писем или писем, которые соответствуют заданным условиям. В блоке доступны следующие параметры:

- **Эл. адреса отправителей** — поле для ввода адресов электронной почты, письма с которых будут обезвреживаться.
- **Эл. адреса получателей** — поле для ввода адресов электронной почты, письма на которые будут обезвреживаться.
- **Обезвреживать заблокированные письма** — флажок, который позволяет включить обезвреживание для заблокированных писем.

Карантин

Для источника, работающего в блокирующем режиме, вы можете включить отправку заблокированных писем в карантин. В этом случае письма не удаляются безвозвратно, а помещаются в карантин. До окончания периода хранения писем в карантине вы можете проанализировать их содержимое и, если признаете их безопасными, переслать адресатам.

Уведомления о блокировке писем

Для источника, работающего в блокирующем режиме, вы можете включить отправку уведомлений о блокировке писем. В блоке доступны следующие параметры настройки уведомлений:

- **Уведомлять** — позволяет выбрать, кого требуется уведомлять: **Только отправителя**, **Только получателей** или **Отправителя и получателей**.
- **Почтовые домены** — поле для ввода имен почтовых доменов. Уведомления будут отправляться только на адреса электронной почты, относящиеся к этим доменам.
- **URL-адрес веб-интерфейса PT Email Security** — поле для ввода адреса, который будет указан в ссылках на результаты проверки. Формат: `http(s)://<Доменное имя или IP-адрес>`.
- **Язык по умолчанию** — раскрывающийся список для выбора языка уведомлений. Указанный язык будет использоваться, если не поддерживается язык почтового клиента.

Блокировка подозрительных файлов

Для источника, работающего в блокирующем режиме, в этом блоке вы можете выбрать, какие еще файлы, кроме опасных, нужно блокировать.

Потенциально опасные файлы — флажок позволяет включить блокировку файлов, которые являются рекламным ПО, выполняют подозрительные действия в ОС или представляют другую угрозу.

Пользовательские правила определения опасных и потенциально опасных файлов

При проверке файлов PT Email Security выявляет различные свойства файлов и по ряду признаков устанавливает для них [метки](#) (см. приложение Г). В этом блоке параметров вы можете настроить дополнительные пользовательские правила, по которым PT Email Security будет относить файлы к опасным или потенциально опасным объектам в зависимости от их свойств.

Внимание! Артефакты поведенческого анализа не проверяются по пользовательским правилам определения файлов с угрозами.

Примечание. Для источника, работающего в блокирующем режиме, вы можете включить блокировку потенциально опасных файлов в блоке **Блокировка подозрительных файлов**.

Правила настраиваются отдельно для каждого источника. В блоке расположены:

- Кнопка **Добавить** для [добавления пользовательского правила](#) (см. раздел 14.7).
- Кнопка **Вставить правило** для добавления правила, скопированного из параметров проверки этого же или другого источника.
- Таблица со списком добавленных правил. При необходимости вы можете отключать и включать правила.

Примечание. По кнопке  в строке правила вы можете изменить это правило, по кнопке  — скопировать, по кнопке  — удалить.

Для каждого правила вы можете указать название, описание и настроить следующие параметры определения опасных и потенциально опасных файлов:

- **Назначаемый уровень опасности** — переключатель для выбора назначаемого файлу уровня опасности: **Опасный** или **Потенциально опасный**.
- **Считать опасными (потенциально опасными)** — переключатель для выбора способа определения содержащих угрозу файлов:
 - **Только файлы со всеми указанными признаками** — к файлам с угрозами будут отнесены файлы, которые соответствуют всем указанным ниже признакам.
 - **Все файлы, кроме файлов с указанными признаками** — к файлам с угрозами будут отнесены файлы, которые не соответствуют хотя бы одному из указанных признаков.
- **Типы файлов** — раскрывающийся список для выбора типов и форматов файлов.

Примечание. Если в поле **Типы файлов** указано несколько значений, файл будет отнесен к файлам с угрозами, если относится к одному из указанных типов или форматов (по логическому правилу ИЛИ). То же самое относится к полям **Маски имен файлов**, **Маски MIME-типов**, **Метки**.

- **Маски имен файлов** — поле для ввода имен и масок имен файлов.

- **Маски MIME-типов** — поле для ввода MIME-типов и масок MIME-типов файлов, например `application/xml, text/*`.
- **Метки** — раскрывающийся список для выбора меток файлов (список недоступен для варианта **Все файлы, кроме файлов с указанными признаками**).

Использовать тестовые YARA-правила

Если включено средство проверки по пользовательским YARA-правилам, для проверки объектов используются действующие YARA-правила. Дополнительно для отладки новых YARA-правил вы можете включить проверку объектов по тестовым YARA-правилам. Результат такой проверки отображается в карточке объекта, но не влияет на вердикт по объекту.

Проверка архивов

В этом блоке вы можете настроить параметры проверки архивов. Доступны следующие параметры:

- **Глубина распаковки архивов** — поле для ввода максимального количества вложенных друг в друга архивов, которые будут распаковываться при проверке. Если распаковывать архивы не требуется, вы можете ввести 0, тогда архивы будут проверяться как обычные файлы. Увеличение глубины распаковки архивов снижает скорость проверки.
- **Определять как потенциально опасные** — в этом блоке параметров вы можете указать признаки архивов, по которым PT Email Security будет относить их к потенциально опасным:
 - **Зашифрованные и нераспакованные архивы** — защищенные паролем архивы, для которых не удалось подобрать пароль.
 - **Архивы с превышенной глубиной распаковки** — архивы, содержащие вложенные архивы, количество которых превышает значение, указанное в параметре **Глубина распаковки архивов**.

Извлечение ссылок из объектов

При включении параметра из поступающих от источников объектов будут извлекаться ссылки и проверяться по индикаторам компрометации.

Проверка контента по извлеченным ссылкам

Если проверка включена, по извлеченным из объектов ссылкам скачивается контент и в виде файлов отправляется на проверку. Проверка выполняется только для ссылок, которые не являются индикаторами компрометации и соответствуют указанным вами параметрам.

В блоке доступны следующие параметры для фильтрации ссылок:

- **Доменные имена, IP-адреса узлов и подсетей для проверки контента** — поле для ввода проверяемых адресов. Контент будет скачиваться и проверяться только по ссылкам на указанные адреса. Эвристический анализ таких ссылок не выполняется. Вы можете

указать имена доменов, поддоменов, IP-адреса узлов или адреса подсетей в формате CIDR. Ссылки на IP-адрес и доменное имя одного и того же ресурса считаются разными ссылками. При вводе адресов вы можете использовать звездочку:

- Если необходимо проверять контент по ссылкам на любые адреса, вы можете ввести *.

Внимание! При пустом поле контент будет проверяться только по тем ссылкам, которые система определит как подозрительные.

- Если необходимо проверять контент по ссылкам на определенный домен, вы можете ввести *<Имя домена>, например *example.com.
- Если необходимо проверять контент по ссылкам на любые поддомены одного домена, вы можете ввести *.<Имя домена>, например *.example.com.

- **Исключаемые доменные имена, IP-адреса узлов и подсетей** — поле для ввода исключаемых адресов. По ссылкам на эти адреса контент скачиваться не будет. Вы можете указать имена доменов, поддоменов, IP-адреса узлов или адреса подсетей в формате CIDR. При вводе адресов вы можете использовать звездочку. Приоритет исключаемых адресов выше приоритета адресов для проверки.
- **Исключаемые категории ссылок** — раскрывающийся список для выбора исключаемых из проверки категорий ссылок. По ссылкам, отнесенным к этим категориям, контент проверяться не будет. Если ссылке присвоена какая-то дополнительная категория, кроме выбранных, контент по ссылке будет проверен. Список категорий ссылок совпадает с перечнем устанавливаемых для ссылок [меток \(см. приложение Г\)](#).
- **Включить эвристику** — при установленном флажке контент будет проверяться по ссылкам, которые система определит как подозрительные.
- **Ограничить количество ссылок для скачивания до** — при установленном флажке вы можете указать количество ссылок в задании, по которым будет скачиваться и проверяться контент. При снятом флажке контент будет проверяться по всем извлеченным в задании ссылкам.

Пользовательские правила определения опасных и потенциально опасных ссылок

При проверке ссылок PT Email Security выполняет категоризацию ссылок и устанавливает для них соответствующие [метки \(см. приложение Г\)](#). В этом блоке параметров вы можете настроить пользовательские правила, по которым PT Email Security будет относить ссылки к опасным или потенциально опасным объектам в зависимости от их категорий. Правила настраиваются отдельно для каждого источника. В блоке расположены:

- Кнопка **Добавить** для [добавления пользовательского правила \(см. раздел 14.10\)](#).
- Кнопка **Вставить правило** для добавления правила, скопированного из параметров проверки этого же или другого источника.
- Таблица со списком добавленных правил. При необходимости вы можете отключать и включать правила.

Примечание. По кнопке  в строке правила вы можете изменить это правило, по кнопке  — скопировать, по кнопке  — удалить.

Для каждого правила вы можете указать название, описание и настроить следующие параметры определения опасных и потенциально опасных ссылок:

- **Назначаемый уровень опасности** — переключатель для выбора назначаемого ссылкам уровня опасности: **Опасный** или **Потенциально опасный**.
- **Считать опасными (потенциально опасными)** — переключатель для выбора способа определения содержащих угрозу ссылок:
 - **Только ссылки указанных категорий** — к ссылкам с угрозами будут отнесены ссылки указанных ниже категорий.
 - **Все ссылки, кроме ссылок указанных категорий** — к ссылкам с угрозами будут отнесены ссылки, не относящиеся ни к одной из указанных категорий.
- **Категории ссылок** — раскрывающийся список для выбора категорий ссылок.

Сохранение файлов без угроз

При включенном параметре в хранилище сохраняются все файлы, в том числе файлы без обнаруженных угроз. При отключении параметра в хранилище будут сохраняться только опасные и потенциально опасные файлы, а также файлы с ошибками.

Внимание! После отключения сохранения файлов без угроз в хранилище вы не сможете выполнить повторную проверку этих файлов.

Поведенческий анализ

При включении параметра вы сможете настроить поведенческий анализ файлов. Такой анализ выполняется только для [некоторых типов файлов \(см. приложение А\)](#). В ходе поведенческого анализа PT Email Security помещает файл в изолированную операционную систему, развернутую в виртуальной машине из указанного вами образа VM, запускает его и имитирует взаимодействие пользователя с этим файлом. Для выявления угроз PT Email Security анализирует действия файла при его запуске или открытии, включая сетевую активность, изменения системных настроек и реестра, запуск процессов, а также создание, изменение и удаление файлов.

Результат поведенческого анализа каждого файла сохраняется в оперативной памяти сервера PT Email Security в течение 48 часов. Если в течение этого времени такой же файл повторно поступает на поведенческий анализ в том же образе VM с такими же параметрами, повторный анализ файла не выполняется, в этом случае используется результат предыдущей проверки. Это позволяет снизить нагрузку на систему.

Для настройки поведенческого анализа файлов необходимо задать правила, по которым PT Email Security будет выполнять анализ. Для разных типов и форматов файлов можно создать отдельные правила с индивидуальными параметрами анализа. В правилах необходимо указать параметры анализа и выбрать образ VM. Рекомендуется выбирать образы VM только с теми

ОС, которые используются в вашей организации. Если файл подпадает под несколько правил, то поведенческий анализ будет выполнен несколько раз с параметрами, указанными в каждом из правил.

Правила поведенческого анализа настраиваются отдельно для каждого источника. В блоке расположены:

- Кнопка **Добавить** для [добавления правила поведенческого анализа \(см. раздел 14.12\)](#).
- Кнопка **Вставить правило** для добавления правила поведенческого анализа, скопированного из параметров проверки этого же или другого источника.
- Таблица со списком добавленных правил. При необходимости вы можете отключать и включать правила.

Примечание. По кнопке  в строке каждого правила вы можете изменить это правило, по кнопке  — скопировать, по кнопке  — удалить.

Для каждого правила вы можете указать название, описание и настроить следующие параметры поведенческого анализа файлов:

- **Образ виртуальной машины** — раскрывающийся список для выбора образа VM.
- **Типы проверяемых файлов** — раскрывающийся список для выбора типов и форматов файлов, которые требуется проверять методом поведенческого анализа в выбранном образе (список доступен после выбора образов VM). Если вы выбрали файлы PDF или файлы офисных форматов, появятся дополнительные блоки параметров.
- **Файлы PDF** — в этом блоке параметров вы можете настроить, какие файлы PDF необходимо проверять методом поведенческого анализа. Вы можете выбрать проверку всех файлов или только файлов, которые зашифрованы, защищены от выполнения с ними каких-либо действий, содержат внедренные объекты (OLE) или сценарии JavaScript, в которых настроены действия при открытии файла (OpenActions) или другие действия (Actions). Если при чтении файла PDF возникнет ошибка (например, если файл поврежден), он также будет проверен методом поведенческого анализа.
- **Файлы офисных форматов** — в этом блоке параметров вы можете настроить, какие файлы офисных форматов необходимо проверять методом поведенческого анализа. Вы можете выбрать проверку всех файлов или только файлов, которые зашифрованы, содержат внедренные объекты (OLE), используют элементы ActiveX, содержат запросы к внешним данным, используют внешний шаблон, функции динамического обмена данными (DDE), содержат настроенные действия (Actions) или надстройки Office. Если при чтении файла возникнет ошибка (например, если файл поврежден), он также будет проверен методом поведенческого анализа. Параметры применяются к файлам OpenDocument и Microsoft Office.
- **Продолжительность наблюдения за файлом** — поля для ввода максимального времени поведенческого анализа в минутах и секундах. Время анализа не должно превышать 10 минут. При проверке архивов это время анализа каждого файла из архива. При выборе значения необходимо учитывать объем и скорость потока файлов в сочетании с производительностью аппаратных ресурсов.

Примечание. Для расчета продолжительности наблюдения за файлом вы можете использовать следующие рекомендации: если файлы приложений проверяются N минут, то презентации, таблицы и документы будут проверяться $1 + N/2$ минут, а файлы PDF — $0,5 + N/3$ минут. Например, если для файлов приложений вы указали продолжительность наблюдения 4 минуты, то для презентаций, таблиц и документов рекомендуется указать 3 минуты, а для файлов PDF — примерно 2 минуты.

- **Расшифровывать и анализировать HTTPS-трафик** — при установленном флажке для расшифровки защищенного HTTPS-трафика между проверяемым файлом и внешними узлами используется собственный сертификат PT Email Security. Если необходимо выявить вредоносное ПО, которое проверяет подлинность сертификатов и прекращает свою активность при обнаружении подмены, вы можете снять флажок.
- **Отключить запись видео** — установка флажка позволяет отключить запись видео поведения файлов в ОС. При снятии флажка видео записывается, но при этом увеличивается нагрузка на систему.

Поведенческий анализ с автоматическим выбором образа

Параметр доступен только для источников типа MaxPatrol EDR. При его включении можно настроить поведенческий анализ файлов с автоматическим выбором образа VM. Для этого необходимо задать правила, по которым PT Email Security будет выполнять анализ. Для разных типов и форматов файлов можно создать отдельные правила с индивидуальными параметрами анализа.

Примечание. Для источников типа MaxPatrol EDR можно одновременно использовать оба варианта поведенческого анализа: с автоматическим выбором образа VM и с фиксированным образом VM.

В правилах анализа с автоматическим выбором образа VM можно указать нескольких образов. Рекомендуется выбирать образы только с теми ОС, которые применяются в вашей организации. Для анализа файла будет выбран образ VM с той же версией ОС, из которой он был получен MaxPatrol EDR, либо максимально близкой к ней по архитектуре. Если файл подходит под несколько правил, используется правило с наиболее подходящим образом VM.

В остальном порядок настройки поведенческого анализа с автоматическим выбором образа VM не отличается от настройки анализа с фиксированным образом VM.

Прекращать проверку для всего задания

При включении поведенческого анализа, для увеличения скорости выполнения заданий PT Email Security может прекращать проверку объектов задания в следующих случаях:

- **Если обнаружен опасный файл** — при установке флажка задание будет прекращено в случае обнаружения хотя бы одного опасного объекта.
- **Если обнаружен потенциально опасный файл** — при установке флажка задание будет прекращено в случае обнаружения хотя бы одного потенциально опасного объекта.

Антифишинг и антиспам

Параметр доступен только для источников типа «Почтовый шлюз безопасности». При его включении письма будут проверяться на наличие признаков фишинга и спама. Дополнительно вы можете настроить проверку IP-адресов и доменных имен, найденных в заголовках и ссылках, по спискам DNS-блокировок.

Примечание. По умолчанию для разрешения адресов, проверяемых по DNS-спискам блокировок, используется DNS-сервер кластера Kubernetes, развернутого в PT Email Security. При необходимости вы можете [указать DNS-серверы вашей организации \(см. раздел 11.1\)](#).

Доступны следующие параметры:

- **Проверять IP-адреса по DNSBL** — при установке флажка по указанным спискам проверяются IP-адреса, извлеченные из заголовков писем.
- **Проверять имена доменов по DNSBL** — при установке флажка по указанным спискам проверяются имена доменов, извлеченные из ссылок в письмах и из адресов электронной почты, указанных в заголовках писем.

По ссылкам **Изменить** вы можете отключить проверку по отдельным спискам DNS-блокировок или добавить дополнительные списки.

14.3. Настройка правил приема писем для почтового шлюза безопасности

Прием писем по правилам доступен только для источников типа «Почтовый шлюз безопасности».

С помощью правил приема писем вы можете настроить действия при запросе подключения к почтовому шлюзу в зависимости от IP-адреса SMTP-клиента. Подключение может быть сразу отклонено, принято для получения писем или принято при выполнении условий подключения. Если для адреса SMTP-клиента не удалось подобрать правило, применяется правило по умолчанию. По этому правилу все письма отклоняются (вы можете изменить действие при запросе). Если адрес подпадает под несколько правил, используется правило, у которого выше приоритет.

Перед настройкой правил приема писем вам необходимо указать список доменов электронной почты получателей, для которых почтовый шлюз будет принимать письма. Если домен не указан в списке, письмо отклоняется шлюзом.

Правила приема писем настраиваются отдельно для каждого источника. Для настройки приема писем по правилам вам необходимо добавить правила приема писем, настроить их приоритет и указать домены принимаемой почты.

Для настройки правил приема писем предназначена вкладка **Правила приема писем** в карточке источника. Карточка источника открывается при нажатии на панель с информацией об источнике на странице **Источники**.

Правила приема писем
Параметры проверки
Правила обработки писем
Задания

+ Добавить
Вставить правило

	Название	Действие при запросе подключения	IP-адреса SMTP-клиента
☒	1 Акцепт	Принять	192.0.2.0/24
☒	2 Check	Принять при выполнении условий	203.0.113.0/24
☐	3 Правило по умолчанию	Отклонить	0.0.0.0/0

Домены принимаемой почты
Шлюз будет обрабатывать только письма, поступившие на указанные почтовые домены.

mail.ru ×
yandex.ru ×

Сохранить

Рисунок 21. Вкладка **Правила приема писем**

В верхней части вкладки расположена таблица с правилами приема писем. В панели инструментов расположены:

- Кнопка **Добавить** для добавления нового правила.
- Кнопка **Вставить правило** для добавления скопированного правила.

В таблице с правилами приема писем вы можете включать или отключать отдельные правила. По кнопкам и в строке правила вы можете изменить приоритет этого правила, по кнопке — изменить правило, по кнопке — скопировать, по кнопке — удалить.

Таблица содержит следующие столбцы с информацией о правилах:

- **Название.**
- **Действие при запросе подключения.**
- **IP-адреса SMTP-клиента** — IP-адреса узлов и подсетей, с которых разрешено подключение.

В нижней части вкладки расположена панель **Домены принимаемой почты** со списком доменов электронной почты получателей, для которых принимаются письма.

Ввод доменов принимаемой почты

По умолчанию список доменов принимаемой почты пуст, все письма отклоняются.

► Чтобы настроить список доменов принимаемой почты:

1. В главном меню выберите **Источники**.
2. Нажмите на панель с информацией об источнике.
Откроется карточка источника.
3. Выберите вкладку **Правила приема писем**.
4. В блоке параметров **Домены принимаемой почты** введите имена доменов.
5. Нажмите кнопку **Сохранить**.

Настройка правил приема писем

Если правила не добавлены, применяется правило по умолчанию. Согласно этому правилу все подключения отклоняются и письма не принимаются (вы можете изменить действие при запросе).

► Чтобы добавить правило приема писем:

1. В главном меню выберите **Источники**.
2. Нажмите на панель с информацией об источнике.
Откроется карточка источника.
3. Выберите вкладку **Правила приема писем**.
4. Нажмите кнопку **Добавить**.
Откроется окно **Добавление правила**.
5. В поле **Название** введите название правила.
6. В поле **IP-адреса узлов и подсетей SMTP-клиента** введите адреса и маски подсетей SMTP-клиентов, для которых применяется правило.
7. В раскрывающемся списке **Действие при запросе подключения** выберите действие:
 - Если требуется принимать подключения и письма, выберите **Принять**.
 - Если требуется отклонять подключения, выберите **Отклонить**.
 - Если требуется проверять параметры запроса на подключение, выберите **Принять при выполнении условий**.
8. Если вы выбрали **Принять при выполнении условий**, настройте проверяемые условия (см. ниже).
9. Нажмите кнопку **Добавить**.
10. Используя кнопки **↑** и **↓** в строке правила, настройте его приоритет.
11. Нажмите кнопку **Сохранить**.

► Чтобы скопировать правило приема писем:

1. В главном меню выберите **Источники**.
2. Нажмите на панель с информацией об источнике.
Откроется карточка источника.
3. Выберите вкладку **Правила приема писем**.
4. В строке правила, которое вы хотите скопировать, нажмите .
5. Нажмите кнопку **Вставить правило**.
Откроется окно **Добавление правила**.
6. Настройте параметры правила приема писем.
7. Нажмите кнопку **Добавить**.
8. Используя кнопки  и  в строке правила, настройте его приоритет.
9. Нажмите кнопку **Сохранить**.

► Чтобы изменить правило приема писем:

1. В главном меню выберите **Источники**.
2. Нажмите на панель с информацией об источнике.
Откроется карточка источника.
3. Выберите вкладку **Правила приема писем**.
4. В строке правила, которое вы хотите изменить, нажмите .
- Откроется окно **Изменение правила**.
5. Измените параметры правила приема писем.
6. Нажмите кнопку **Изменить**.
7. Нажмите кнопку **Сохранить**.

► Чтобы удалить правило приема писем:

1. В главном меню выберите **Источники**.
2. Нажмите на панель с информацией об источнике.
Откроется карточка источника.
3. Выберите вкладку **Правила приема писем**.
4. В строке правила, которое вы хотите удалить, нажмите  и подтвердите удаление.
5. Нажмите кнопку **Сохранить**.

Условия, проверяемые при запросе подключения

Настраивать условия, проверяемые при запросе подключения к почтовому шлюзу от SMTP-клиента, вы можете при добавлении, копировании или изменении правила с действием при запросе **Принять при выполнении условий**. Для каждого условия выделен блок параметров, в котором вы можете включить или отключить проверку этого условия и по кнопке  настроить параметры проверки. Блоки с условиями разделены на группы с помощью заголовков:

- **TLS-шифрование** — для настройки требований к TLS-шифрованию:
 - **Требуется шифрование TLS** — позволяет настроить требование к наличию такого шифрования на стороне SMTP-клиента. Вы можете выбрать минимальную версию TLS у клиента и настроить код и сообщение ответа при отклонении письма.
- **Команда HELO/EHLO** — для настройки требований к команде HELO/EHLO:
 - **Требуется команда HELO/EHLO** — позволяет настроить требование к наличию такой команды в запросе от SMTP-клиента. Вы можете настроить код и сообщение ответа при отклонении письма.
 - **Доменное имя SMTP-клиента указано в формате FQDN** — позволяет настроить требование к формату доменного имени SMTP-клиента, передаваемому в команде HELO/EHLO. Вы можете настроить код и сообщение ответа при отклонении письма.
 - **Доменное имя SMTP-клиента соответствует хотя бы одному регулярному выражению в белом списке** — позволяет настроить проверку доменного имени SMTP-клиента, передаваемого в команде HELO/EHLO, по белому списку. Вы можете настроить белый список имен доменов, код и сообщение ответа при отклонении письма.
 - **Доменное имя SMTP-клиента не соответствует ни одному из регулярных выражений в черном списке** — позволяет настроить проверку доменного имени SMTP-клиента, передаваемого в команде HELO/EHLO, по черному списку. Вы можете настроить черный список имен доменов, код и сообщение ответа при отклонении письма.
- **Команда MAIL FROM** — для настройки требований к команде MAIL FROM:
 - **Эл. адрес отправителя не соответствует ни одному из регулярных выражений в черном списке** — позволяет настроить проверку электронного адреса отправителя письма по черному списку. Вы можете настроить черный список адресов, код и сообщение ответа при отклонении письма.
- **Команда RCPT TO** — для настройки требований к команде RCPT TO:
 - **Эл. адрес получателя не соответствует ни одному из регулярных выражений в черном списке** — позволяет настроить проверку электронного адреса получателя письма по черному списку. Вы можете настроить черный список адресов, код и сообщение ответа при отклонении письма.

- **Аутентификация электронной почты** — для настройки требований к аутентификации электронной почты:
 - **Пройдена проверка SPF** — позволяет настроить проверку адреса SMTP-клиента по SPF-записям домена электронной почты отправителя, если такие записи доступны. Вы можете настроить при каком результате проверка не будет пройдена, код и сообщение ответа при отклонении письма.
 - **Письмо содержит валидную подпись DKIM** — проверка подписи DKIM всегда включена и выполняется при наличии такой подписи у принимаемого письма.
 - **Пройдена проверка DMARC** — проверка подлинности письма по DMARC всегда включена.
- **Антиспам по DNSBL** — для настройки требований к параметрам антиспама по DNSBL.
 - **Адрес SMTP-клиента отсутствует в списках DNS-блокировок** — позволяет настроить проверку адреса SMTP-клиента по спискам DNS-блокировок. Вы можете указать, какие списки требуется использовать при проверке, код и сообщение ответа при отклонении письма.

14.4. Настройка обработки писем по правилам

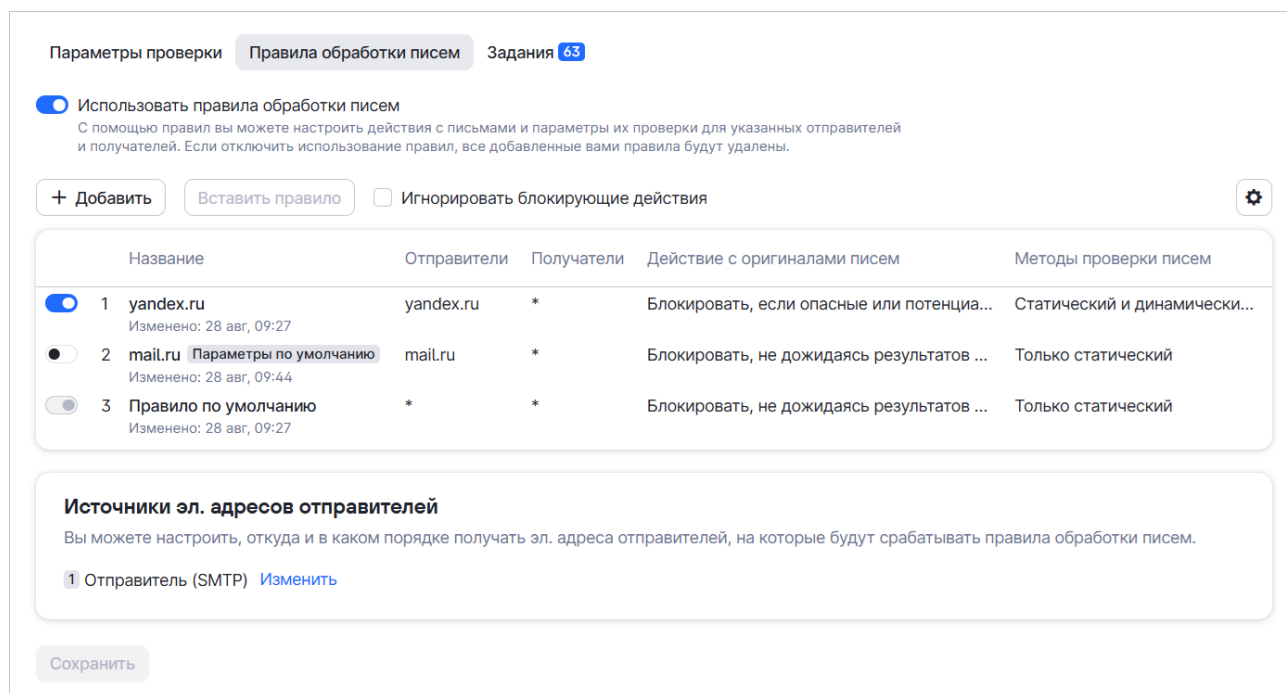
Обработка писем по правилам доступна для источников «Почтовый сервер в режиме фильтрации», «Почтовый сервер в режиме зеркалирования», «Сервер Microsoft Exchange с установленным агентом» и «Почтовый шлюз безопасности».

С помощью правил обработки вы можете настроить действия с поступившими на проверку письмами (блокировать или пропускать) и методы их проверки в зависимости от адресов или доменов электронной почты отправителей и получателей. Если для письма не удалось подобрать правило, используется правило по умолчанию. Если письмо подпадает под несколько правил, используется правило, у которого выше приоритет.

Правила обработки писем настраиваются отдельно для каждого источника. Для настройки обработки писем по правилам вам необходимо:

1. Включить обработку писем по правилам.
2. Настроить правило обработки писем по умолчанию.
3. Добавить необходимые правила обработки писем и настроить их приоритет.
4. Настроить источники адресов отправителей, которые будут учитываться в правилах.

Для настройки обработки писем по правилам предназначена вкладка **Правила обработки писем** в карточке источника. Карточка источника открывается при нажатии на панель с информацией об источнике на странице **Источники**.

Рисунок 22. Вкладка **Правила обработки писем**

В верхней части вкладки вы можете включить или отключить обработку писем по правилам.

В центральной части вкладки расположена таблица с правилами обработки писем. В панели инструментов расположены:

- Кнопка **Добавить** для добавления нового правила.
- Кнопка **Вставить правило** для добавления скопированного правила.
- Флажок **Игнорировать блокирующие действия** для отключения блокировки писем во всех правилах. При установке флажка в таблице будут выделены правила, для которых отключена блокировка писем.
- Кнопка  для выбора столбцов, которые должны отображаться в таблице.

В таблице с правилами обработки писем вы можете включать или отключать отдельные правила. По кнопкам  и  в строке правила вы можете изменить приоритет этого правила, по кнопке  — изменить правило, по кнопке  — скопировать, по кнопке  — удалить.

В зависимости от вашего выбора таблица может содержать следующие столбцы с информацией о правилах:

- **Название** — название правила.
- **Отправители** — адреса и домены электронной почты отправителей писем, для которых применяется правило.
- **Получатели** — адреса и домены электронной почты получателей писем, для которых применяется правило.

- **Действие с оригиналами писем** — действие с письмами, подпадающими под правило.
- **Методы проверки писем** — методы проверки писем, подпадающих под правило.
- **Максимальное время ожидания результатов проверки** — максимальное время, на которое будут задерживаться письма для проверки, если в правиле выбрано действие с блокировкой писем.
- **Действия с заблокированными письмами** — действие с письмами, подпадающими под правило, если в правиле выбрано действие с блокировкой писем.
- **Сообщение получателю** — сообщение, отправляемое по электронной почте получателям при блокировке письма.
- **Сообщение отправителю** — сообщение, отправляемое по электронной почте отправителю при блокировке письма.

В нижней части вкладки расположена панель **Источники эл. адресов отправителей** со списком источников адресов отправителей, которые используются при работе правил. По ссылке **Изменить** вы можете выбрать источники и настроить их приоритет.

Включение и отключение обработки писем по правилам

При включении обработки писем по правилам из параметров проверки источника пропадет возможность выбора режима проверки и некоторые другие параметры проверки (исключения, обезвреживание писем, карантин и блокировка подозрительных файлов). Эти параметры настраиваются с помощью правил обработки писем.

Внимание! При отключении обработки писем по правилам все добавленные вами правила будут удалены.

► Чтобы включить или отключить обработку писем по правилам:

1. В главном меню выберите **Источники**.
2. Нажмите на панель с информацией об источнике.
Откроется карточка источника.
3. Выберите вкладку **Правила обработки писем**.
4. Включите или отключите использование правил обработки писем.
5. Нажмите кнопку **Сохранить**.

Параметры правила обработки писем

Настраивать параметры правила обработки писем вы можете при добавлении, копировании или изменении правила. Доступны следующие параметры:

- **Название** — поле для ввода названия правила. Может содержать только буквы латинского алфавита, цифры, дефис, точку, двоеточие, запятую, пробел, знак подчеркивания и &.
- **Эл. адреса и домены отправителей** — поле для ввода адресов и доменов электронной почты отправителей писем, для которых применяется правило. При вводе вы можете использовать маски с подстановочными знаками:
 - Если необходимо проверять письма с любых адресов, вы можете ввести *.
 - Если необходимо проверять любые письма с одного домена, вы можете ввести *. <Имя домена>, например *.example.com.
 - Если необходимо проверять письма без адреса отправителя, вы можете ввести <>.
- **Эл. адреса и домены получателей** — поле для ввода адресов и доменов электронной почты получателей писем, для которых применяется правило. При вводе вы также можете использовать маски с подстановочными знаками.
- **Использовать параметры правила по умолчанию** — при установке флажка для правила будут использоваться параметры обработки писем, указанные в правиле по умолчанию.
- **Действие с оригиналами писем** — раскрывающийся список для выбора действия с письмами, попадающими под правило. Доступны следующие действия:
 - **Блокировать, если опасные.**
 - **Блокировать, если опасные или потенциально опасные.**
 - **Блокировать, не дожидаясь результатов проверки.**
 - **Пропускать, не дожидаясь результатов проверки.**
- **Методы проверки писем** — блок параметров для настройки методов проверки писем, попадающих под правило. Доступны следующие методы:
 - **Статический и динамический анализ.**

Не ждать завершения динамического анализа — при установленном флажке, если в письме не обнаружено угроз, оно пропускается в информационную систему сразу после завершения статического анализа.
 - **Только статический.**
 - **Без проверки.**
- **Максимальное время ожидания результатов проверки** — если в правиле выбрано действие с блокировкой писем, в это поле можно ввести максимальное время, на которое будут задерживаться письма для проверки. По истечении этого времени письма пропускаются в информационную систему до вынесения вердикта.

- **Действия с заблокированными письмами** — если в правиле выбрано действие с блокировкой писем, с помощью этого параметра можно выбрать действие с заблокированными письмами. Доступны следующие действия:
 - **Помещать в карантин.**
 - **Удалять.**
- **Сообщение при блокировке письма** — блок параметров для выбора сообщений, которые отправляются по электронной почте отправителям и получателям писем в случае блокировки. Доступны следующие варианты:
 - **Уведомление о блокировке.**
 - **Отправить безвредную копию письма** (только для получателей).
 - **Ничего не отправлять.**

Настройка правил обработки писем

Правила можно добавлять, изменять, включать или отключать и удалять. Добавленное ранее правило можно скопировать для того же или другого источника.

- ▶ Чтобы добавить правило обработки писем:
 1. В главном меню выберите **Источники**.
 2. Нажмите на панель с информацией об источнике.
Откроется карточка источника.
 3. Выберите вкладку **Правила обработки писем**.
 4. Нажмите кнопку **Добавить**.
Откроется окно **Добавление правила**.
 5. Настройте параметры правила обработки писем.
 6. Нажмите кнопку **Добавить**.
 7. Используя кнопки **↑** и **↓** в строке правила, настройте его приоритет.
 8. Нажмите кнопку **Сохранить**.
- ▶ Чтобы скопировать правило обработки писем:
 1. В главном меню выберите **Источники**.
 2. Нажмите на панель с информацией об источнике.
Откроется карточка источника.
 3. Выберите вкладку **Правила обработки писем**.
 4. В строке правила, которое вы хотите скопировать, нажмите .

5. Нажмите кнопку **Вставить правило**.

Откроется окно **Добавление правила**.

6. Настройте параметры правила обработки писем.

7. Нажмите кнопку **Добавить**.

8. Используя кнопки  и  в строке правила, настройте его приоритет.

9. Нажмите кнопку **Сохранить**.

► Чтобы изменить правило обработки писем:

1. В главном меню выберите **Источники**.

2. Нажмите на панель с информацией об источнике.

Откроется карточка источника.

3. Выберите вкладку **Правила обработки писем**.

4. В строке правила, которое вы хотите изменить, нажмите .

Откроется окно **Изменение правила**.

5. Измените параметры правила обработки писем.

6. Нажмите кнопку **Изменить**.

7. Нажмите кнопку **Сохранить**.

► Чтобы удалить правило обработки писем:

1. В главном меню выберите **Источники**.

2. Нажмите на панель с информацией об источнике.

Откроется карточка источника.

3. Выберите вкладку **Правила обработки писем**.

4. В строке правила, которое вы хотите удалить, нажмите  и подтвердите удаление.

5. Нажмите кнопку **Сохранить**.

Настройка источников адресов отправителей

► Чтобы настроить источники адресов отправителей:

1. В главном меню выберите **Источники**.

2. Нажмите на панель с информацией об источнике.

Откроется карточка источника.

3. Выберите вкладку **Правила обработки писем**.

4. В панели **Источники эл. адресов отправителей** перейдите по ссылке **Изменить**.
5. Включите нужные источники адресов отправителей.
6. Используя кнопки  и  в строке источника, настройте приоритет каждого источника.
7. Нажмите кнопку **Изменить**.
8. Нажмите кнопку **Сохранить**.

14.5. Настройка блокирующего режима проверки писем

Блокирующий режим проверки писем доступен для источников с типами «Почтовый сервер в режиме фильтрации» и «Сервер Microsoft Exchange с установленным агентом», если ваша лицензия предусматривает работу PT Email Security в таком режиме. Если для источника включена обработка писем по правилам, настройка блокирующего режима выполняется с помощью правил обработки писем.

В блокирующем режиме проверки, поступившие на проверку письма блокируются PT Email Security до окончания проверки. В зависимости от вынесенного вердикта письма пропускается в информационную систему или удаляется (или помещается в карантин).

Включение блокирующего режима

► Чтобы включить блокирующий режим проверки писем:

1. В главном меню выберите **Источники**.
2. В панели с информацией об источнике перейдите по ссылке **Параметры проверки**.
3. В блоке параметров **Режим проверки** выберите **Блокирующий**.
4. Выберите метод анализа, по результатам которого письма можно пропускать в информационную систему:
 - Если по результатам динамического анализа, выберите **После завершения динамического анализа**.
 - Если достаточно результатов статического анализа, выберите **Не дожидаясь завершения динамического анализа**.
5. Если необходимо изменить время проверки письма, в поле **Максимальное время ожидания результатов проверки** измените это время.

Внимание! Не рекомендуется снижать время проверки. Если указанного времени будет недостаточно для завершения проверки, письмо будет доставлены получателям непроверенным. Это может привести к проникновению в информационную систему писем с угрозами.

6. Нажмите кнопку **Сохранить**.

Блокирующий режим проверки писем включен.

Настройка исключений для блокирующего режима

Вы можете указать адреса получателей, для которых письма не будут блокироваться, независимо от результатов проверки.

► Чтобы добавить адреса получателей в исключения блокирующего режима:

1. В главном меню выберите **Источники**.
2. В панели с информацией об источнике перейдите по ссылке **Параметры проверки**.
3. В блоке параметров **Исключения** в поле **Эл. адреса получателей** введите адреса.
4. Нажмите кнопку **Сохранить**.

Адреса получателей добавлены в исключения блокирующего режима.

Настройка обезвреживания писем

Вы можете настроить обезвреживание писем для блокирующего режима проверки. При обезвреживании письма:

- Текст письма преобразуется из форматов HTML и RTF в обычный текст.
- Удаляются все ссылки из письма, а на их месте отображается текст [ссылка удалена].
- Удаляются все вложения.

Предусмотрены два типа обезвреживания писем:

- Безусловное. Все письма, поступающие на почтовый сервер организации, будут обезвреживаться до проведения каких-либо проверок. При этом перемещение писем в карантин недоступно, а оригиналы писем удаляются.

Внимание! При выборе безусловного типа обезвреживания возможна потеря важной информации из писем.

- По условиям. Вы можете настроить параметры, по которым будут обезвреживаться письма. При добавлении адресов электронной почты отправителей или получателей, обезвреженные письма будут отправляться получателям. Оригиналы писем удаляются или помещаются в карантин, если для источника включена отправка опасных писем в карантин и письмо считается опасным по результатам проверки. При обезвреживании писем, которые должны быть заблокированы, уведомления о блокировке не отправляются.

► Чтобы настроить обезвреживание писем:

1. В главном меню выберите **Источники**.
2. В блоке параметров **Обезвреживание писем** включите обезвреживание.
3. Выберите тип обезвреживания:
 - Если требуется обезвреживать все письма, выберите вариант **Все**.

- Если требуется обезвреживать письма по настраиваемым параметрам, выберите вариант **По условиям**.
- 4. Если вы выбрали обезвреживание по условиям, вы можете настроить следующие параметры:
 - Если требуется обезвреживать письма от определенных отправителей, укажите их адреса в поле **Эл. адреса отправителей**.
 - Если требуется обезвреживать письма для определенных получателей, укажите их адреса в поле **Эл. адреса получателей**.
 - Если требуется обезвреживать письма, которые должны быть заблокированы, установите флажок **Обезвреживать заблокированные письма**.
- 5. Нажмите кнопку **Сохранить**.

Обезвреживание писем настроено.

Включение карантина

Вы можете включить карантин для заблокированных писем. Вместо удаления заблокированные письма будут помещаться в карантин на время, указанное в основных параметрах PT Email Security. В течение этого времени вы можете проанализировать содержимое писем и, если признаете их безопасными, [переслать их адресатам](#) (см. раздел 10.3).

► Чтобы включить карантин для заблокированных писем:

1. В главном меню выберите **Источники**.
2. В панели с информацией об источнике перейдите по ссылке **Параметры проверки**.
3. В блоке параметров **Карантин** включите карантин.
4. Нажмите кнопку **Сохранить**.

Карантин для заблокированных писем включен.

Настройка почтовых уведомлений о блокировке писем

Вы можете настроить отправку почтовых уведомлений о блокировке писем. Уведомления отправляются на адреса электронной почты отправителя и получателей заблокированного письма. Вы можете ограничить отправку уведомлений, указав домены серверов электронной почты. В этом случае уведомления будут отправляться только на адреса, относящиеся к указанным доменам.

► Чтобы настроить уведомления о блокировке писем:

1. В главном меню выберите **Источники**.
2. В панели с информацией об источнике перейдите по ссылке **Параметры проверки**.

3. В блоке параметров **Уведомления о блокировке писем** включите уведомления.
4. Выберите, кого необходимо уведомлять о блокировке письма: только отправителя, только получателей или отправителя и получателей.
5. Если необходимо ограничить отправку уведомлений, в поле **Почтовые домены** введите доменные имена, к которым должны относиться адреса электронной почты получателей уведомлений.

Например, если необходимо отправлять уведомления только на адреса, заканчивающиеся на @example.com, в поле нужно ввести example.com. Если необходимо также отправлять уведомления на адреса, заканчивающиеся на @support.example.com, в поле нужно добавить адрес поддомена support.example.com.

6. В поле **URL-адрес веб-интерфейса PT Email Security** введите адрес в формате `http(s)://<Доменное имя или IP-адрес>`.
Этот адрес будет использоваться в уведомлениях в ссылках на результаты проверки.
7. В раскрывающемся списке **Язык по умолчанию** выберите язык уведомлений для случаев, когда язык почтового клиента не поддерживается.
8. Если необходимо изменить текст сообщения в уведомлениях, в поле **Сообщение для отправителя** или **Сообщение для получателей** введите текст сообщения.
9. Нажмите кнопку **Сохранить**.

Уведомления о блокировке писем настроены.

Включение блокировки потенциально опасных файлов

Вы можете включить блокировку писем с потенциально опасными файлами.

► Чтобы включить блокировку потенциально опасных файлов:

1. В главном меню выберите **Источники**.
2. В панели с информацией об источнике перейдите по ссылке **Параметры проверки**.
3. В блоке параметров **Блокировка подозрительных файлов** установите флажок **Потенциально опасные файлы**.
4. Нажмите кнопку **Сохранить**.

Блокировка потенциально опасных файлов включена.

14.6. Настройка блокирующего режима проверки файлов

Блокирующий режим проверки файлов доступен для источников с типами «Папка-шлюз», если ваша лицензия предусматривает работу PT Email Security в таком режиме.

В блокирующем режиме проверки, поступившие на проверку файлы блокируются PT Email Security до окончания проверки. В зависимости от вынесенного вердикта файлы пропускаются в информационную систему или удаляются.

Включение блокирующего режима

- Чтобы включить блокирующий режим проверки файлов:
1. В главном меню выберите **Источники**.
 2. В панели с информацией об источнике перейдите по ссылке **Параметры проверки**.
 3. В блоке параметров **Режим проверки** выберите **Блокирующий**.
 4. Выберите метод анализа, по результатам которого файл можно пропускать в информационную систему:
 - Если по результатам динамического анализа, выберите **После завершения динамического анализа**.
 - Если достаточно результатов статического анализа, выберите **Не дожидаясь завершения динамического анализа**.
 5. Нажмите кнопку **Сохранить**.
- Блокирующий режим проверки файлов включен.

Включение блокировки потенциально опасных файлов

- Чтобы включить блокировку потенциально опасных файлов:
1. В главном меню выберите **Источники**.
 2. В панели с информацией об источнике перейдите по ссылке **Параметры проверки**.
 3. В блоке параметров **Блокировка подозрительных файлов** установите флажок **Потенциально опасные файлы**.
 4. Нажмите кнопку **Сохранить**.
- Блокировка потенциально опасных файлов включена.

14.7. Настройка пользовательских правил определения файлов с угрозами

При проверке файлов PT Email Security выявляет различные свойства файлов и по ряду признаков устанавливает для них [метки \(см. приложение Г\)](#). С помощью пользовательских правил вы можете указать свойства файлов, по которым PT Email Security будет относить их к опасным или потенциально опасным объектам.

Внимание! Артефакты поведенческого анализа не проверяются по пользовательским правилам определения файлов с угрозами.

Правила настраиваются отдельно для каждого источника. Пользовательские правила можно добавлять, изменять и удалять. Добавленное ранее правило вы можете скопировать для того же или другого источника.

Добавление пользовательского правила

► Чтобы добавить пользовательское правило определения файлов с угрозами:

1. В главном меню выберите **Источники**.
2. В панели с информацией об источнике нажмите кнопку **Параметры проверки**.
3. В блоке параметров **Пользовательские правила определения опасных и потенциально опасных файлов** нажмите кнопку **Добавить**.
Откроется окно **Добавление правила**.
4. В поле **Название** введите название правила.
5. Выберите назначаемый уровень опасности файлов: **Опасный** или **Потенциально опасный**.
6. В блоке параметров **Считать опасными (потенциально опасными)** выберите способ определения содержащих угрозу файлов:
 - Если требуется относить к файлам с угрозами файлы, которые соответствуют всем указанным ниже признакам, выберите **Только файлы со всеми указанными признаками**.
 - Если требуется относить к файлам с угрозами все файлы, которые не соответствуют хотя бы одному из указанных признаков, выберите **Все файлы, кроме файлов с указанными признаками**.
7. Укажите признаки файлов:
 - В раскрывающемся списке **Типы файлов** выберите типы и форматы файлов.

Примечание. Если вы указали несколько значений, файл будет отнесен к файлам с угрозами, если относится к одному из указанных типов или форматов (по логическому правилу ИЛИ). То же самое относится к полям **Маски имен файлов**, **Маски MIME-типов**, **Метки**.

- В поле **Маски MIME-типов** последовательно введите отдельные MIME-типы и маски MIME-типов, например `application/xml`, `text/*`.
- Если вы выбрали вариант **Только файлы со всеми указанными признаками**, в раскрывающемся списке **Метки** выберите метки файлов.

Примечание. По ссылке **Объекты, подходящие под правило** вы можете просмотреть список уже проверенных файлов, которые подходят под правило.

8. Нажмите кнопку **Добавить**.

9. Нажмите кнопку **Сохранить**.

Пользовательское правило определения файлов с угрозами добавлено.

Копирование пользовательского правила

► Чтобы скопировать пользовательское правило определения файлов с угрозами:

1. В главном меню выберите **Источники**.
2. В панели с информацией об источнике нажмите кнопку **Параметры проверки**.
3. В блоке параметров **Пользовательские правила определения опасных и потенциально опасных файлов** в строке правила, которое вы хотите скопировать, нажмите .
4. Нажмите кнопку **Вставить правило**.
Откроется окно **Добавление правила**.
5. В поле **Название** измените название правила.
6. Нажмите кнопку **Добавить**.
7. Нажмите кнопку **Сохранить**.

Пользовательское правило определения файлов с угрозами скопировано.

Изменение пользовательского правила

► Чтобы изменить пользовательское правило определения файлов с угрозами:

1. В главном меню выберите **Источники**.
2. В панели с информацией об источнике нажмите кнопку **Параметры проверки**.
3. В блоке параметров **Пользовательские правила определения опасных и потенциально опасных файлов** в строке правила, которое вы хотите изменить, нажмите .
4. Измените правило.
5. Нажмите кнопку **Изменить**.
6. Нажмите кнопку **Сохранить**.

Пользовательское правило определения файлов с угрозами изменено.

Удаление пользовательского правила

► Чтобы удалить пользовательское правило определения файлов с угрозами:

1. В главном меню выберите **Источники**.
2. В панели с информацией об источнике нажмите кнопку **Параметры проверки**.
3. В блоке параметров **Пользовательские правила определения опасных и потенциально опасных файлов** в строке правила, которое вы хотите удалить, нажмите  и подтвердите удаление.
4. Нажмите кнопку **Сохранить**.

Пользовательское правило определения файлов с угрозами удалено.

14.8. Настройка проверки архивов

► Чтобы настроить проверку архивов:

1. В главном меню выберите **Источники**.
2. В панели с информацией об источнике перейдите по ссылке **Параметры проверки**.
3. В блоке **Проверка архивов** в поле **Глубина распаковки архивов** укажите до какого уровня вложенности будут распаковываться архивы.
Если необходимо отключить распаковку архивов, введите 0.
4. Укажите какие архивы необходимо относить к потенциально опасным объектам:
 - Если зашифрованные и нераспакованные архивы, установите соответствующий флажок.
 - Если архивы с превышенной глубиной распаковки, установите соответствующий флажок.
5. Нажмите кнопку **Сохранить**.

14.9. Настройка проверки ссылок

Проверка выполняется только для ссылок, которые не являются индикаторами компрометации. По ссылкам скачивается контент и в виде файлов отправляется на проверку.

Для проверки ссылок рекомендуется добавить отдельный прокси-сервер и не использовать для этого прокси-сервер PT Email Security.

► Чтобы настроить проверку ссылок:

1. В главном меню выберите **Источники**.
2. В панели с информацией об источнике нажмите кнопку **Параметры проверки**.
3. В блоке параметров **Извлечение ссылок из объектов** включите извлечение ссылок.

4. В блоке параметров **Проверка контента по извлеченным ссылкам** включите проверку.
5. Укажите, по каким ссылкам необходимо проверять контент:
 - Если необходимо проверять контент по ссылкам на любые адреса, в поле **Доменные имена, IP-адреса узлов и подсетей для проверки контента** введите *.

Внимание! При пустом поле **Доменные имена, IP-адреса узлов и подсетей для проверки контента** контент будет проверяться только по тем ссылкам, которые система определит как подозрительные.

- Если необходимо проверять контент по ссылкам на определенные адреса, в поле **Доменные имена, IP-адреса узлов и подсетей для проверки контента** укажите эти адреса.

Вы можете указать имена доменов, поддоменов, IP-адреса узлов или адреса подсетей в формате CIDR. Контент будет проверяться по ссылкам на адреса, которые точно совпадают с указанными. Ссылки на IP-адрес и доменное имя одного и того же ресурса считаются разными ссылками.

При вводе адресов вы можете использовать звездочку. Если необходимо проверять контент по ссылкам на определенный домен, вы можете ввести ***<Имя домена>**, например *example.com. Если необходимо проверять контент по ссылкам на любые поддомены одного домена, вы можете ввести *.**<Имя домена>**, например *.example.com.

- Если не требуется проверять ссылки, которые PT Email Security определит как подозрительные, снимите флажок **Включить эвристику**.
6. Если ссылки, ведущие на какие-то адреса, проверять не требуется, в поле **Исключаемые доменные имена, IP-адреса узлов и подсетей** укажите эти адреса.

Вы можете указать имена доменов, поддоменов, IP-адреса узлов или адреса подсетей в формате CIDR. Из проверки будут исключены ссылки на адреса, которые точно совпадают с указанными. При вводе адресов вы можете использовать звездочку. Приоритет исключаемых адресов выше приоритета адресов для проверки.

Внимание! Ссылки в письмах могут содержать вредоносные запросы. Чтобы исключить выполнение таких запросов внутри IT-инфраструктуры вашей организации, рекомендуется добавить в исключения адреса внутренние IP-адреса и доменные имена, в том числе IP-адреса и доменные имена узлов PT Email Security.

7. Если необходимо ограничить количество ссылок, проверяемых в одном задании, установите флажок **Ограничить количество ссылок для скачивания до** и введите количество ссылок.

Внимание! Большое количество проверяемых ссылок может значительно увеличить нагрузку на PT Email Security.

8. Нажмите кнопку **Сохранить**.

Проверка ссылок настроена.

14.10. Настройка пользовательских правил определения ссылок с угрозами

При проверке ссылок PT Email Security выполняет их категоризацию. Категории ссылок назначаются с учетом содержания и назначения веб-ресурсов, а также их потенциальной угрозы для информационной безопасности. В зависимости от категорий каждой ссылке присваиваются соответствующие [метки \(см. приложение Г\)](#). С помощью пользовательских правил вы можете указать, ссылки каких категорий нужно относить к опасным или потенциально опасным объектам.

Пользовательские правила определения ссылок с угрозами настраиваются отдельно для каждого источника. Вы можете добавлять, изменять и удалять правила. Добавленное ранее правило вы можете скопировать для того же или другого источника.

Добавление пользовательского правила

Перед добавлением пользовательского правила определения ссылок с угрозами необходимо в параметрах проверки источника включить извлечение ссылок из объектов.

► Чтобы добавить пользовательское правило определения ссылок с угрозами:

1. В главном меню выберите **Источники**.
2. В панели с информацией об источнике нажмите кнопку **Параметры проверки**.
3. В блоке параметров **Пользовательские правила определения опасных и потенциально опасных ссылок** нажмите кнопку **Добавить**.
Откроется окно **Добавление правила**.
4. В поле **Название** введите название правила.
5. Выберите назначаемый уровень опасности ссылок: **Опасный** или **Потенциально опасный**.
6. В блоке параметров **Считать опасными (потенциально опасными)** выберите способ определения содержащих угрозу ссылок:
 - Если требуется относить к ссылкам с угрозами только ссылки, которые относятся к одной из указанных категорий, выберите **Только ссылки указанных категорий**.
 - Если требуется относить к ссылкам с угрозами все ссылки, которые не относятся ни к одной из указанных категорий, выберите **Все ссылки, кроме ссылок указанных категорий**.
7. В раскрывающемся списке **Категории ссылок** выберите категории ссылок.
8. Нажмите кнопку **Добавить**.
9. Нажмите кнопку **Сохранить**.

Пользовательское правило определения ссылок с угрозами добавлено.

Копирование пользовательского правила

► Чтобы скопировать пользовательское правило определения ссылок с угрозами:

1. В главном меню выберите **Источники**.
2. В панели с информацией об источнике нажмите кнопку **Параметры проверки**.
3. В блоке параметров **Пользовательские правила определения опасных и потенциально опасных ссылок** в строке правила, которое вы хотите скопировать, нажмите .
4. Нажмите кнопку **Вставить правило**.
Откроется окно **Добавление правила**.
5. В поле **Название** измените название правила.
6. Нажмите кнопку **Добавить**.
7. Нажмите кнопку **Сохранить**.

Пользовательское правило определения ссылок с угрозами скопировано.

Изменение пользовательского правила

► Чтобы изменить пользовательское правило определения ссылок с угрозами:

1. В главном меню выберите **Источники**.
2. В панели с информацией об источнике нажмите кнопку **Параметры проверки**.
3. В блоке параметров **Пользовательские правила определения опасных и потенциально опасных ссылок** в строке правила, которое вы хотите изменить, нажмите .
4. Измените правило.
5. Нажмите кнопку **Изменить**.
6. Нажмите кнопку **Сохранить**.

Пользовательское правило определения ссылок с угрозами изменено.

Удаление пользовательского правила

► Чтобы удалить пользовательское правило определения ссылок с угрозами:

1. В главном меню выберите **Источники**.
2. В панели с информацией об источнике нажмите кнопку **Параметры проверки**.

3. В блоке параметров **Пользовательские правила определения опасных и потенциально опасных ссылок** в строке правила, которое вы хотите удалить, нажмите  и подтвердите удаление.
4. Нажмите кнопку **Сохранить**.

Пользовательское правило определения ссылок с угрозами удалено.

14.11. Отключение сохранения файлов без угроз в хранилище

По умолчанию PT Email Security сохраняет в хранилище файлы без угроз, поступающие со всех источников. Чтобы избежать быстрого заполнения хранилища при проверке большого количества файлов, вы можете отключить сохранение файлов без угроз.

Внимание! После отключения сохранения файлов без угроз в хранилище вы не сможете выполнить повторную проверку этих файлов.

► Чтобы отключить сохранение файлов без угроз в хранилище:

1. В главном меню выберите **Источники**.
2. В панели с информацией об источнике нажмите кнопку **Параметры проверки**.
3. В блоке параметров **Сохранение файлов без угроз** отключите сохранение файлов в хранилище.
4. Нажмите кнопку **Сохранить**.

Сохранение файлов без угроз в хранилище отключено.

14.12. Настройка правил поведенческого анализа

Вы можете настроить правила, по которым PT Email Security будет проводить поведенческий анализ для различных типов и форматов файлов.

Правила поведенческого анализа настраиваются отдельно для каждого источника. Вы можете добавлять, изменять и удалять правила. Добавленное ранее правило вы можете скопировать для того же или другого источника.

Добавление правила поведенческого анализа

► Чтобы добавить правило поведенческого анализа:

1. В главном меню выберите **Источники**.
2. В панели с информацией об источнике нажмите кнопку **Параметры проверки**.
3. В блоке **Поведенческий анализ** включите анализ.

4. Нажмите кнопку **Добавить**.

Откроется окно **Добавление правила**.

5. Если вы добавляете правило для поведенческого анализа с фиксированным образом VM, в раскрывающемся списке **Образ виртуальной машины** выберите образ для развертывания изолированной операционной системы.
6. Если вы добавляете правило для поведенческого анализа с автоматическим выбором образа VM, в раскрывающемся списке **Образ виртуальной машины** отметьте несколько образов, из которых будет выбираться наиболее подходящий.
7. В раскрывающемся списке **Типы проверяемых файлов** выберите типы и форматы файлов.

Примечание. Для файлов офисных форматов и PDF вы можете указать свойства, при наличии которых файлы необходимо проверять.

8. Если требуется изменить время анализа каждого файла, в поле **Продолжительность наблюдения за файлом** измените время.
9. Если при анализе защищенного трафика не требуется подменять сертификаты, снимите флажок **Расшифровывать и анализировать HTTPS-трафик**.
10. Если не требуется записывать видео действий, выполняемых с файлом, установите флажок **Отключить запись видео**.
11. Нажмите кнопку **Добавить**.
12. Нажмите кнопку **Сохранить**.

Правило поведенческого анализа добавлено.

Копирование правила поведенческого анализа

- Чтобы скопировать правило поведенческого анализа:

1. В главном меню выберите **Источники**.
 2. В панели с информацией об источнике нажмите кнопку **Параметры проверки**.
 3. В блоке параметров **Правила поведенческого анализа** в строке правила, которое вы хотите скопировать, нажмите .
 4. Нажмите кнопку **Вставить правило**.
- Откроется окно **Добавление правила**.
5. Нажмите кнопку **Добавить**.
 6. Нажмите кнопку **Сохранить**.

Правило поведенческого анализа скопировано.

Изменение правила поведенческого анализа

► Чтобы изменить правило поведенческого анализа:

1. В главном меню выберите **Источники**.
2. В панели с информацией об источнике нажмите кнопку **Параметры проверки**.
3. В блоке параметров **Правила поведенческого анализа** в строке правила, которое вы хотите изменить, нажмите .

Откроется окно **Изменение правила**.

4. Измените правило.
5. Нажмите кнопку **Изменить**.
6. Нажмите кнопку **Сохранить**.

Правило поведенческого анализа изменено.

Удаление правила поведенческого анализа

► Чтобы удалить правило поведенческого анализа:

1. В главном меню выберите **Источники**.
2. В панели с информацией об источнике нажмите кнопку **Параметры проверки**.
3. В блоке параметров **Правила поведенческого анализа** в строке правила, которое вы хотите удалить, нажмите  и подтвердите удаление.
4. Нажмите кнопку **Сохранить**.

Правило поведенческого анализа удалено.

15. Просмотр конфигурации PT Email Security

На страницах раздела **Система** → **Конфигурация** вы можете получить общее представление о настроенной конфигурации PT Email Security: об узлах, входящих в конфигурацию, их IP-адресах и ролях, о развернутых на узлах компонентах и подах. Вы также можете оценить работоспособность конфигурации, увидеть, какие из узлов, компонентов или подов не работают или работают частично, и принять решения по улучшению их работоспособности.

Примечание. В PT Email Security используется микросервисная архитектура и контейнеризация приложений на основе технологий containerd и Kubernetes (K8s). Для просмотра докер-контейнеров и докер-образов вы можете использовать утилиты `crictl` и `ctr`. Утилиты доступны на узлах PT Email Security.

В верхней части каждой страницы указаны:

- Статус отказоустойчивого кластера (отображается, если такой кластер настроен).
- Виртуальный IP-адрес отказоустойчивого кластера (отображается, если такой кластер настроен).
- Общее количество узлов для поведенческого анализа файлов и количество доступных узлов (отображается, если часть узлов недоступна).
- Общее количество виртуальных машин, которые можно запустить на всех узлах для поведенческого анализа файлов, и количество доступных для запуска виртуальных машин (отображается, если часть виртуальных машин недоступна).

Содержимое рабочей области зависит от выбранной страницы.

Страница «Компоненты»

Для просмотра информации о компонентах PT Email Security предназначена страница **Система** → **Конфигурация** → **Компоненты**.

Отказоустойчивый кластер

Настроен

Адрес кластера

10.120.10.120

Узлы для поведенческого анализа

1

ВМ для поведенческого анализа

2

Название	↓↑	Тип	↓↑	Узел	↓↑	Пространство имен	↓↑	Работающих подов	↓↑	Статус	↑
vmagent		Служба мониторинга		ptms-astra-all-qa4		monitoring		0 из 1		Не работает	
prometheus-adapter		Служба мониторинга		ptms-astra-all-qa4		monitoring		11 из 12		Работает частично	
telemetry		Служба интеграции		ptms-astra-all-qa4		ptms		2		Работает	
ptioc		Средство проверки		ptms-astra-node3-q...		ptms		2		Работает	
ptcategorizer		Средство проверки		ptms-astra-node3-q...		ptms		2		Работает	
cluster-babysitter		Служба обновления		ptms-astra-all-qa4		ptms		1		Работает	
av-nano		Средство проверки		ptms-astra-node3-q...		ptms		4		Работает	
mc-licensing		Служба		ptms-astra-node3-q...		ptmc		1		Работает	
kube-state-metrics		Служба мониторинга		ptms-astra-all-qa4		monitoring		1		Работает	

Рисунок 23. Страница **Компоненты**

В рабочей области страницы расположена таблица с информацией о компонентах PT Email Security. По кнопке **↓↑** в заголовке любого столбца таблицы вы можете отсортировать компоненты по значениям в этом столбце. Нажимая на заголовок столбца, вы можете отфильтровать содержимое таблицы по значениям в столбце. Для каждого компонента в таблице указаны:

- **Название.**
- **Тип** — назначение компонента.
- **Узел** — название узла, на котором развернут компонент.
- **Пространство имен:**
 - **ptms** — PT Email Security.
 - **ptmc** — PT MC.
 - **monitoring** — подсистема мониторинга работы PT Email Security.
- **Работающих подов** — количество работающих подов и общее количество подов, используемых компонентом.
- **Статус** — один из статусов пода: **Работает**, **Работает частично** или **Не работает**.

Страница «Узлы»

Для просмотра информации о входящих в конфигурацию PT Email Security узлах и ролях этих узлов предназначена страница **Система** → **Конфигурация** → **Узлы**.

Отказоустойчивый кластер

Настроен

Адрес кластера

10.120.10.120

Узлы для поведенческого анализа

1

ВМ для поведенческого анализа

2

ptms-astra-node3

Работает

scan-core

backend

persistent-data

control-plane

IP-адрес

ЦП

ОЗУ

ОС

containerd

Kubernetes

Поды

10.120.4.143

6 ядер

15,62 ГБ

Astra Linux

1.6.20

v1.26.4

30

ptms-astra-node2

Работает

scan-core

backend

persistent-data

control-plane

IP-адрес

ЦП

ОЗУ

ОС

containerd

Kubernetes

Поды

10.120.4.142

6 ядер

15,62 ГБ

Astra Linux

1.6.20

v1.26.4

22

ptms-astra-sandbox

Работает

sandbox

IP-адрес

ЦП

ОЗУ

ОС

containerd

Kubernetes

Xen

Поды

ВМ

10.120.4.149

16 ядер

26,47 ГБ

Astra Linux

1.6.20

v1.26.4

4.16.5

15

2

Рисунок 24. Страница **Узлы**

В рабочей области страницы расположены панели с информацией об узлах, входящих в конфигурацию PT Email Security. Для каждого узла указаны:

- Имя ноды Kubernetes и имя узла (если оно отличается от имени ноды).
- Роли узла. Могут быть настроены следующие роли:
 - **backend** — сервер приложений. На таком сервере могут быть установлены: встроенный PT MC, служба обновлений, служба публичного API и другие компоненты PT Email Security.
 - **control-plane** — основной или резервный узел с управляющей нодой Kubernetes.
 - **persistent-data** — хранилище файлов.
 - **sandbox** — узел для поведенческого анализа.
 - **scan-core** — ядро проверки PT Email Security.
- **IP-адрес** — IP-адрес узла.
- **ЦП** — количество ядер центрального процессора.
- **ОЗУ** — объем памяти.
- **ОС** — версия операционной системы.
- **containerd** — версия среды containerd.
- **Kubernetes** — версия Kubernetes.
- **Xen** — версия гипервизора Xen.

- **Поды** — количество подов, развернутых на узле.
- **ВМ** — количество виртуальных машин, которые можно запустить на узле для поведенческого анализа файлов.
- Статус узла: **Работает**, **Есть ошибки** или **Недоступен**.

Страница «Поды»

Для просмотра информации о подах Kubernetes предназначена страница **Система** → **Конфигурация** → **Поды**.

Отказоустойчивый кластер Настроен		Адрес кластера 10.120.10.120		Узлы для поведенческого анализа 1		ВМ для поведенческого анализа 2	
Имя пода	Компонент	Узел	Перезапусков	Время работы	Работающих контейн...	Статус	
os-installer-xffsn	os-installer	ptms-astra-node3	2	2 д 4 ч	0	Не работает	
prometheus-adapt...	prometheus-adapter	ptms-astra-node3	2	3 нед 5 д	1	Работает	
trace2ml-6746f74c...	trace2ml	ptms-astra-node4	0	3 ч 1 мин	1	Работает	
trace2ml-6746f74c...	trace2ml	ptms-astra-node3	0	3 ч 1 мин	1	Работает	
ptioc-7cc7bb44bc-...	ptioc	ptms-astra-node3	0	3 ч 22 мин	1	Работает	
ptioc-7cc7bb44bc-...	ptioc	ptms-astra-node3	0	3 ч 21 мин	1	Работает	
ptcategorizer-c6d4...	ptcategorizer	ptms-astra-node4	0	3 ч 24 мин	1	Работает	
ptcategorizer-c6d4...	ptcategorizer	ptms-astra-node3	0	3 ч 23 мин	1	Работает	
cluster-babysitter-...	cluster-babysitter	ptms-astra-node4	0	3 ч 26 мин	2	Работает	

Рисунок 25. Страница **Поды**

В рабочей области страницы расположена таблица с информацией о подах Kubernetes. По кнопке  в заголовке любого столбца таблицы вы можете отсортировать поды по значениям в этом столбце. Нажимая на заголовок столбца, вы можете отфильтровать содержимое таблицы по значениям в столбце. Для каждого пода в таблице указаны:

- **Имя**.
- **Компонент** — название компонента, использующего под.
- **Узел** — название узла, на котором развернут под.
- **Перезапусков** — количество перезапусков пода.
- **Время работы** — общее время работы пода.
- **Работающих контейнеров** — количество контейнеров, работающих внутри пода.
- **Статус** — один из статусов пода: **Работает**, **Не работает**.

16. Мониторинг системных ресурсов в Grafana

Для визуализации данных об использовании системных ресурсов на узлах PT Email Security используется средство визуализации и мониторинга данных Grafana с набором стандартных дашбордов. Для работы с Grafana в главном меню вам необходимо выбрать раздел **Система** → **Конфигурация** → **Мониторинг**. Страница Grafana открывается в отдельной вкладке браузера. На странице отображается дашборд, выбранный основным. Работа Grafana одновременно на нескольких вкладках не поддерживается.

Примечание. По умолчанию установлена темная тема оформления интерфейса. Вы можете сменить тему оформления на светлую в параметрах профиля пользователя.

При работе с Grafana вы можете:

- Просматривать информацию на основном дашборде.
- Выбирать для просмотра другие стандартные дашборды.

Инструкции по работе с Grafana вы можете найти в технической документации Grafana.

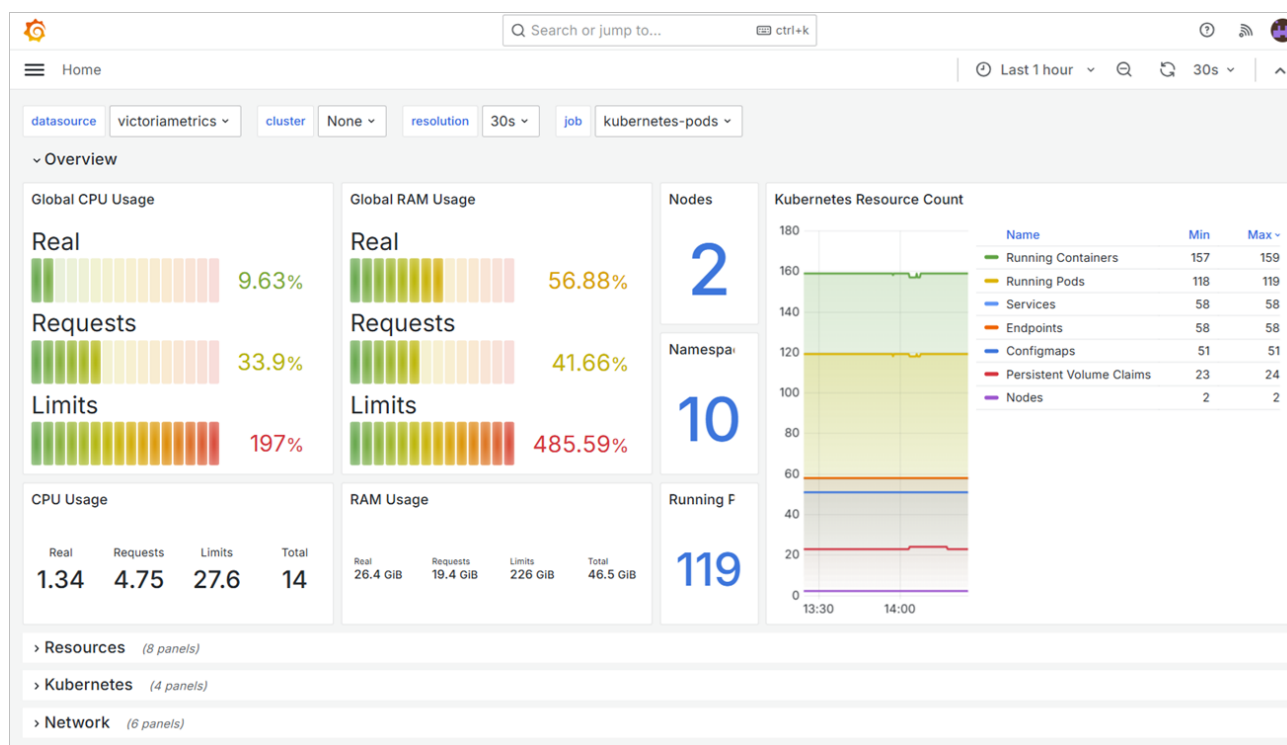


Рисунок 26. Мониторинг системных ресурсов в Grafana

В верхней части страницы расположена панель инструментов с кнопками:

☰ — для открытия боковой панели с главным меню. Используя разделы главного меню, вы можете переходить на страницы Grafana:

- **Home** — для просмотра домашней страницы с основным дашбордом.
- **Starred** — для выбора избранных дашбордов.
- **Dashboards** — для выбора дашбордов для просмотра.
- **Explore** — для создания запросов к источникам данных.
- **Alerting** — для просмотра настроенных уведомлений.

🕒 — для выбора периода времени, за который отображаются данные на виджетах.

↻ — для обновления данных на виджетах.

⌵ — для настройки автоматического обновления данных на виджетах.

В рабочей области страницы отображаются виджеты выбранного вами дашборда. Виджеты сгруппированы в раскрывающиеся блоки.

Назначение стандартных дашбордов

Для мониторинга обработки объектов в PT Email Security предназначены дашборды:

- **Product / Rabbitmq / Queues** — предоставляет детализированные данные об очередях сообщений компонента RabbitMQ, включая общее количество очередей, динамику изменения количества сообщений в очередях, а также скорость поступления, доставки и подтверждения сообщений.
- **Product / Gateway / BCC** — предназначен для мониторинга обработки писем от источников типа «Почтовый сервер в режиме фильтрации» и «Почтовый сервер в режиме зеркалирования».

В блоке **Current rates** отображаются график изменения режимов работы источников во времени. Для каждого источника фиксируются переходы между блокирующим и пассивным режимами, что позволяет отследить стабильность их работы.

В блоке **Incoming Emails Stats** отображается статистика приема писем. Представлен график по времени, отражающий динамику изменения количества писем, полученных от каждого источника. Также представлены диаграммы, показывающие распределение общего количества писем по источникам и их типам.

В блоке **Processed Emails Stats** отображается статистика обработки писем.

Представлена гистограмма, показывающая распределение количества писем по времени их обработки, что позволяет оценить общую нагрузку и типичную продолжительность обработки письма.

Также представлены графики, отражающие динамику изменения во времени следующих показателей: количества писем, для которых выполнено определенное действие (пропущено, заблокировано), и количества писем, обработанных без таких действий; количества писем с определенными статусом, вердиктом и причиной вердикта (отдельные графики для пропущенных и заблокированных писем и для писем, обработанных без таких действий); количества обработанных писем от каждого источника.

Примечание. Письмо считается заблокированным, если оно заблокировано хотя бы для одного получателя. На графиках и диаграммах для писем, обработанных без выполнения каких-либо действий, учитываются письма только от источников типа «Почтовый сервер в режиме зеркалирования».

Кроме того, представлены диаграммы, показывающие распределение общего числа обработанных писем: по именам источников (отдельные диаграммы для пропущенных и заблокированных писем и для писем, обработанных без таких действий); по действиям (пропущено, заблокировано или обработано без таких действий); по статусам обработки (успешно или с ошибкой); отдельно для писем без задания на проверку — по действиям (пропущено или заблокировано).

В блоке **Errors Stats** отображается статистика ошибок при обработке писем.

Представлены графики, отражающие динамику изменения во времени количества ошибок с определенными типами и кодами. Также приведены диаграммы, показывающие распределение общего количества ошибок по типам и кодам. Даны отдельные графики и диаграммы для ошибок, возникших при попытке отправить письмо на внешний почтовый сервер, и ошибок, возвращенных удаленным сервером в ответ на отправку.

Для фильтрации данных в панели инструментов дашборда можно выбрать тип и название источника.

- **Product / BA Queue** — дашборд предназначен для мониторинга состояния и производительности модуля поведенческого анализа.

В блоке **Current queue size** отображаются текущее количество файлов в очереди на поведенческий анализ (добавленных и проверяемых), продолжительность анализа, количество запущенных для анализа ВМ, история изменения длины очереди и распределение накладных расходов по временным диапазонам.

Блок **Total stats** содержит статистику запусков поведенческого анализа за выбранный период: распределение по источникам, типам файлов и образам ВМ, количество ошибок и показатели эффективности кэширования.

В блоке **Rates in time** представлены графики по времени, отражающие динамику ошибок, накладных расходов, использования ВМ, запусков поведенческого анализа по источникам, типам файлов и образам ВМ, а также показатели активности кэша и количества успешно завершённых запусков.

Для фильтрации данных в панели инструментов дашборда можно выбрать источники, образы ВМ и типы файлов.

Для мониторинга узлов PT Email Security предназначен дашборд:

- **Node Exporter Full** — предоставляет детализированные данные о состоянии узлов PT Email Security, включая загрузку центрального процессора, использование памяти ОЗУ, состояние файловых систем и сетевой трафик.

Для мониторинга компонентов PT Email Security предназначены дашборды:

- **RabbitMQ-Overview** — дашборд предоставляет сводную информацию о работе компонента RabbitMQ, включая количество очередей, сообщений, соединений, каналов и узлов, а также скорость поступления, доставки, подтверждения и повторной отправки сообщений. Кроме того, дашборд предоставляет данные об использовании компонентом системных ресурсов, включая память ОЗУ, дисковое пространство, файловые дескрипторы и сокеты.
- **VictoriaMetrics — cluster** — предоставляет информацию о загрузке центрального процессора, использовании памяти ОЗУ и дискового пространства в кластере системы VictoriaMetrics.
- **VictoriaMetrics — vmagent** — отображает информацию о работе агента сбора данных vmagent системы VictoriaMetrics, включая объем передаваемых данных и задержки их обработки.

В PT Email Security используется микросервисная архитектура и контейнеризация приложений на основе технологий containerd и Kubernetes. Для мониторинга работы кластера Kubernetes предназначены дашборды:

- **kube-state-metrics-v2** — отображает состояние объектов Kubernetes, включая узлы, поды, развертывания (Deployments), наборы подов с состоянием (Statefulset), контейнеры, автоскейлеры, задания и постоянные хранилища.
- **Kubernetes / System / API Server** — предназначен для мониторинга производительности API-сервера Kubernetes, включая нагрузку на обработку запросов и задержки операций.
- **Kubernetes / Views / Global** — предоставляет сводную информацию о загрузке ресурсов и состоянии всех компонентов кластера Kubernetes (основной дашборд по умолчанию).
- **Kubernetes / Views / Namespaces** — показывает использование ресурсов и количество активных подов в разрезе пространств имен.
- **Kubernetes / Views / Nodes** — отображает данные о производительности и загрузке узлов Kubernetes, включая центральный процессор, память ОЗУ и сетевые ресурсы.
- **Kubernetes / Views / Pods** — предоставляет информацию о статусе подов, использовании ими ресурсов и возможных причинах перезапусков.
- **Kubernetes Cluster Monitoring** — отображает данные о состоянии кластера Kubernetes, включая работу сервисов и использование вычислительных ресурсов.
- **Kubernetes Metrics — Deployments vs StatefulSets vs DaemonSets** — предназначен для просмотра информации об использовании ресурсов различных типов развертываний в Kubernetes, включая загрузку центрального процессора, использование памяти ОЗУ, дискового пространства, сетевого ввода-вывода и количество недоступных реплик.

17. О технической поддержке

Гарантийная поддержка доступна для всех владельцев действующих лицензий на PT Email Security в течение периода предоставления обновлений и включает в себя следующий набор услуг.

Предоставление доступа к обновленным версиям продукта

Обновления продукта выпускаются в порядке и в сроки, определяемые Positive Technologies. Positive Technologies предоставляет обновленные версии продукта в течение оплаченного периода получения обновлений, указанного в бланке лицензии приобретенного продукта Positive Technologies.

Positive Technologies не производит установку обновлений продукта в рамках гарантийной поддержки и не несет ответственности за инциденты, возникшие в связи с некорректной или несвоевременной установкой обновлений продукта.

Восстановление работоспособности продукта

Специалист Positive Technologies проводит диагностику заявленного сбоя и предоставляет рекомендации для восстановления работоспособности продукта. Восстановление работоспособности может заключаться в выдаче рекомендаций по установке продукта заново с потенциальной потерей накопленных данных либо в восстановлении версии продукта из доступной резервной копии (резервное копирование должно быть настроено заблаговременно). Positive Technologies не несет ответственности за потерю данных в случае неверно настроенного резервного копирования.

Примечание. Помощь оказывается при условии, что конечным пользователем продукта соблюдены все аппаратные, программные и иные требования и ограничения, описанные в документации к продукту.

Устранение ошибок и дефектов в работе продукта в рамках выпуска обновленных версий

Если в результате диагностики обнаружен дефект или ошибка в работе продукта, Positive Technologies обязуется включить исправление в ближайшие возможные обновления продукта (с учетом релизного цикла продукта, приоритета дефекта или ошибки, сложности требуемых изменений, а также экономической целесообразности исправления). Сроки выпуска обновлений продукта остаются на усмотрение Positive Technologies.

Рассмотрение предложений по доработке продукта

При обращении с предложением по доработке продукта необходимо подробно описать цель такой доработки. Вы можете поделиться рекомендациями по улучшению продукта и оптимизации его функциональности. Positive Technologies обязуется рассмотреть все предложения, однако не принимает на себя обязательств по реализации каких-либо

доработок. Если Positive Technologies принимает решение о доработке продукта, то способы ее реализации остаются на усмотрение Positive Technologies. Заявки принимаются [на портале технической поддержки](#).

Портал технической поддержки

[На портале технической поддержки](#) вы можете круглосуточно создавать и обновлять заявки и читать новости продуктов.

Для получения доступа к portalу технической поддержки нужно создать учетную запись, используя адрес электронной почты в официальном домене вашей организации. Вы можете указать другие адреса электронной почты в качестве дополнительных. Добавьте в профиль название вашей организации и контактный телефон — так нам будет проще с вами связаться.

Поддержка на портале предоставляется на русском и английском языках.

Условия предоставления гарантийной поддержки

Для получения гарантийной поддержки необходимо оставить заявку [на портале технической поддержки](#) и предоставить следующие данные:

- номер лицензии на использование продукта;
- файлы журналов и наборы диагностических данных, которые требуются для анализа;
- снимки экрана.

Positive Technologies не берет на себя обязательств по оказанию услуг гарантийной поддержки в случае вашего отказа предоставить запрашиваемую информацию или отказа от внедрения предоставленных рекомендаций.

Если заказчик не предоставляет необходимую информацию по прошествии 20 календарных дней с момента ее запроса, специалист технической поддержки имеет право закрыть заявку. Оказание услуг может быть возобновлено по вашей инициативе при условии предоставления запрошенной ранее информации.

Услуги по гарантийной поддержке продукта не включают в себя услуги по переустановке продукта, решение проблем с операционной системой, инфраструктурой заказчика или сторонним программным обеспечением.

Заявки могут направлять уполномоченные сотрудники заказчика, владеющего продуктом на законном основании (включая наличие действующей лицензии). Специалисты заказчика должны иметь достаточно знаний и навыков для сбора и предоставления диагностической информации, необходимой для решения заявленной проблемы.

Услуги по гарантийной поддержке оказываются в отношении поддерживаемых версий продукта. Информация о поддерживаемых версиях содержится в «Политике поддержки версий программного обеспечения» и (или) иных информационных материалах, размещенных на официальном веб-сайте Positive Technologies.

Время реакции и приоритизация заявок

При получении заявки ей присваивается регистрационный номер, специалист службы технической поддержки классифицирует ее (присваивает тип и уровень значимости) и выполняет дальнейшие шаги по ее обработке.

Время реакции рассчитывается с момента получения заявки до первичного ответа специалиста технической поддержки с уведомлением о взятии заявки в работу. Время реакции зависит от уровня значимости заявки. Специалист службы технической поддержки оставляет за собой право переопределить уровень значимости в соответствии с приведенными ниже критериями. Указанные сроки являются целевыми, но возможны отклонения от них по объективным причинам.

Таблица 5. Время реакции на заявку

Уровень значимости заявки	Критерии значимости заявки	Время реакции на заявку
Критический	Аварийные сбои, приводящие к невозможности штатной работы продукта (исключая первоначальную установку) либо оказывающие критически значимое влияние на бизнес заказчика	До 4 часов
Высокий	Сбои, проявляющиеся в любых условиях эксплуатации продукта и оказывающие значительное влияние на бизнес заказчика	До 8 часов
Средний	Сбои, проявляющиеся в специфических условиях эксплуатации продукта либо не оказывающие значительного влияния на бизнес заказчика	До 8 часов
Низкий	Вопросы информационного характера либо сбои, не влияющие на эксплуатацию продукта	До 8 часов

Указанные часы относятся к рабочему времени (рабочие дни с 9:00 до 18:00 UTC+3) специалистов технической поддержки. Под рабочим днем понимается любой день за исключением субботы, воскресенья и дней, являющихся официальными нерабочими днями в Российской Федерации.

Обработка и закрытие заявок

По мере рассмотрения заявки и выполнения необходимых действий специалист службы поддержки сообщает вам:

- о ходе диагностики по заявленной проблеме и ее результатах;
- планах выпуска обновленной версии продукта (если требуется для устранения проблемы).

Если по итогам обработки заявки необходимо внести изменения в продукт, Positive Technologies включает работы по исправлению в ближайшее возможное плановое обновление продукта (с учетом релизного цикла продукта, приоритета дефекта или ошибки, сложности требуемых изменений, а также экономической целесообразности исправления). Сроки выпуска обновлений продукта остаются на усмотрение Positive Technologies.

Специалист закрывает заявку, если:

- предоставлены решение или возможность обойти проблему, не влияющие на критически важную функциональность продукта (по усмотрению Positive Technologies);
- диагностирован дефект продукта, собрана техническая информация о дефекте и условиях его воспроизведения, исправление дефекта запланировано к выходу в рамках планового обновления продукта;
- заявленная проблема вызвана программным обеспечением или оборудованием сторонних производителей, на которые не распространяются обязательства Positive Technologies;
- заявленная проблема классифицирована специалистами Positive Technologies как неподдерживаемая.

Примечание. Если продукт приобретался вместе с аппаратной платформой в виде программно-аппаратного комплекса (ПАК), решение заявок, связанных с ограничением или отсутствием работоспособности аппаратных компонентов, происходит согласно условиям и срокам, указанным в гарантийных обязательствах (гарантийных талонах) на такие аппаратные компоненты.

Приложение А. Типы файлов, отправляемых на поведенческий анализ

PT Email Security может выполнять поведенческий анализ файлов только тех типов и форматов, которые указаны в таблице.

Таблица 6. Типы файлов, отправляемых на поведенческий анализ

Типы файлов	Форматы файлов, поддерживаемые в образах	
	Windows	ОС семейства Linux
Файлы данных		
Табличные данные	IQY, SLK	—
Исполняемые файлы		
Java	JAR, JNLP	JAR
Мультиплатформенные скрипты	JS ³ , PL, PY	JS ³ , PL, PY
Документы HTML	CHM, HTA	—
Для Windows	BAT, CMD, EXE, JS, JSE, PS1, SCR, VBE, VBS, WSF	—
Для семейства Linux	—	ELF, SH
Установочные пакеты	APPX, APPXBUNDLE, MSI, MSIX, MSIXBUNDLE	DEB, RPM
Файлы офисных приложений		
Документы	DOC, DOCM, DOCX, DOT, DOTM, DOTX, ODT, RTF, WBK	DOC, DOCM, DOCX, DOT, DOTM, DOTX, ODF, ODG, ODT, OTT, RTF
Таблицы	ODS, XLA, XLAM, XLS, XLSB, XLSM, XLSX, XLT, XLTM, XLTX	ODS, OTS, XLA, XLAM, XLS, XLSB, XLSM, XLSX, XLT, XLTM, XLTX
Презентации	ODP, POT, POTM, POTX, PPA, PPAM, PPS, PPSM, PPSX, PPT, PPTM, PPTX, SLDM, SLDX	ODP, PPA, POT, POTM, POTX, PPS, PPSM, PPSX, PPT, PPTM, PPTX, SLDX
Файлы PDF	PDF	PDF
Файлы Microsoft Publisher	PUB	—

³ Файлы этого типа не отправляются на поведенческий анализ, если они получены от источников с типом «ICAP-сервер» или «PT NAD».

Типы файлов	Форматы файлов, поддерживаемые в образах	
	Windows	ОС семейства Linux
Системные файлы		
Библиотеки и драйверы	DLL	—
Другие системные файлы	LNK, URL	—
Файлы приложений		
Базы данных	ACCDB, ACCDE, ACCDT, MDB, MDE	—

Приложение Б. Прикладные протоколы, поддерживаемые PT Email Security при поведенческом анализе файлов

В этом разделе перечислены протоколы прикладного уровня, которые поддерживает PT Email Security при поведенческом анализе файлов.

Таблица 7. Обнаруживаемые прикладные протоколы

Обозначение	Протокол
amqp	Advanced Message Queuing Protocol (amqp.org)
bgp	Border Gateway Protocol (RFC4271)
bittorrent	Протокол BitTorrent (bittorrent.org)
canon-bjnp	Протокол обнаружения сервиса LAN, используемый в принтерах и сканерах Canon (canon.com)
clickhouse	Протокол системы управления базами данных ClickHouse (clickhouse.com)
db2-drda	Db2 Distributed Relational Database Architecture (ibm.com)
dcerpc	Distributed Computing Environment / Remote Procedure Call
dhcp	Dynamic Host Configuration Protocol (RFC 2131)
dhcpv6	Dynamic Host Configuration Protocol for IPv6 (RFC 3315)
dns	Domain Name System (RFC 1034)
drweb	Протокол продукта Dr.Web Enterprise Security Suite (drweb.ru)
dtls	Datagram Transport Layer Security (RFC 6347)
elasticsearch	Протокол системы Elasticsearch (elastic.co)
encrypted	Неизвестный зашифрованный протокол
facebook	Протокол сети Facebook ⁴ (developers.facebook.com)
falcongaze	Протокол продукта Falcongaze SecureTower Agent (falcongaze.com)
fb-zero	Протокол сети Facebook Zero ⁴ (0.facebook.com)
ftp	File Transfer Protocol (RFC 959)
guardant	Протокол продукта Guardant Net (guardant.ru)

⁴ Facebook, Instagram и WhatsApp — продукты компании Meta, которая, в соответствии с законодательством Российской Федерации, признана экстремистской организацией и запрещена в России.

Обозначение	Протокол
http	Hypertext Transfer Protocol
icap	Internet Content Adaptation Protocol (RFC 3507)
imap	Internet Message Access Protocol (RFC 3501)
infowatch	Протокол продукта InfoWatch Device Monitor (infowatch.ru)
isakmp	Internet Security Association and Key Management Protocol (RFC 2408)
jrmf	Java Remote Method Invocation Protocol (oracle.com)
kafka	Протокол платформы Apache Kafka (kafka.apache.org)
kerberos	Протокол аутентификации Kerberos (RFC 4120)
ksn	Протокол сети Kaspersky Security Network (kaspersky.ru/ksn)
ldap	Lightweight Directory Access Protocol (RFC 4510)
llmnr	Link-Local Multicast Name Resolution (RFC 4795)
lotus	Протокол платформы HCL Notes (ранее IBM Notes и Lotus Notes)
mc-nmf	Net.TCP Port Sharing (docs.microsoft.com)
mdns	Multicast DNS (RFC 6762)
memcache	Протокол системы Memcached (memcached.org)
mongodb	Протокол системы управления базами данных MongoDB (docs.mongodb.com)
ms-scom	Протокол программы System Center Operations Manager (docs.microsoft.com)
ms-update	Протокол утилиты Windows Update Delivery Optimization (docs.microsoft.com)
mysql	Протокол системы управления базами данных MySQL (dev.mysql.com)
nat-t	NAT Traversal
nbns	NetBIOS Name Server (RFC 1001)
nfs	Network File System (RFC 1094)
ntlm	NT LAN Manager (docs.microsoft.com)
ntp	Network Time Protocol (ntp.org)
openvpn	Протокол технологии OpenVPN (openvpn.net)
oracle-tns	Oracle TNS (Transparent Network Substrate, протокол компании Oracle)
p2p-dc	Протокол Direct Connect

Обозначение	Протокол
pop3	Post Office Protocol 3 (RFC 1081)
postgresql	Протокол системы управления базами данных PostgreSQL (postgresql.org)
pptp	Point-to-Point Tunneling Protocol (RFC 2637)
printer-pjl	Протокол Printer Job Language (hp.com)
printer-ps	Протокол печати PostScript (adobe.com)
quic	UDP-Based Multiplexed and Secure Transport, экспериментальный протокол Google (tools.ietf.org/html/draft-ietf-quic-transport-27)
radius	Remote Authentication Dial In User Service (RFC 2865)
redis	Протокол системы управления базами данных Redis (redis.io)
rexec	Протокол приложения REXEC (ibm.com)
rfb	Remote Framebuffer (RFC 6143)
rlogin	BSD Rlogin (RFC 1282)
rsync	Протокол утилиты rsync (rsync.samba.org)
rtcp	Real-Time Transport Protocol (RFC 3550)
rtsp	Real-Time Streaming Protocol (RFC 7826)
sip	Session Initiation Protocol (RFC 3261)
skinny-voip	Skinny Client Control Protocol (cisco.com)
skype	Протокол программы Skype (skype.com)
smb	Server Message Block (docs.microsoft.com)
smb-mailslot	Server Message Block Mailslot (docs.microsoft.com)
smtp	Simple Mail Transfer Protocol (RFC 5321)
snmp	Simple Network Management Protocol
socks5	SOCKS 5 (RFC 1928)
splunk	Протокол платформы Splunk (splunk.com)
ssdp	Simple Service Discovery Protocol
ssh	Secure Shell (RFC 4251)
stakhanovets	Протокол DLP-системы компании «Стахановец» (stakhanovets.ru/dlp)
stun	Session Traversal Utilities for NAT (RFC 3489)
stun-apple	
stun-classic	

Обозначение	Протокол
syslog	Протокол системного журнала (RFC 5424)
tds	Tabular Data Stream (docs.microsoft.com)
teamviewer	Протокол программы TeamViewer (teamviewer.com)
telnet	Telnet (RFC 854)
tftp	Trivial File Transfer Protocol (RFC 1350)
thrift	Протокол фреймворка Apache Thrift (thrift.apache.org)
tls	Transport Layer Security (RFC 8446)
trueconf	Протокол системы TrueConf (trueconf.ru)
umeye-app	Протокол приложения UMEye (umeye.com)
viber	Протокол приложения Viber (viber.com)
vipaks-data	Протокол передачи видео компании «Випакс» (vipaks.ru)
vipnet	Протокол системы ViPNet VPN (infotecs.ru)
vipnet-mftp	
vipnet-sync	
vpn_kontinent	Протокол комплекса шифрования «Континент» (securitycode.ru)
vmware	Протокол компании VMware (vmware.com)
whatsapp	Протокол приложения WhatsApp ⁴ (whatsapp.com)
wireguard	WireGuard (wireguard.com)
ws-discovery	Web Services Dynamic Discovery (specs.xmlsoap.org)
xmpp	Extensible Messaging and Presence Protocol (xmpp.org)
zabbix	Протокол системы Zabbix (zabbix.com)
zmtp	ZeroMQ Message Transport Protocol (zeromq.org)
zmtp_v2	

Приложение В. Базовые образы VM

В PT Email Security доступны образы VM с различными версиями Windows и ОС семейства Linux. Информация о доступных образах отображается на странице **Средства проверки** → **Поведенческий анализ** → **Образы виртуальных машин** → **Управление образами**.

Образы VM операционных систем семейства Windows

В PT Email Security доступны образы VM со следующими версиями Windows:

- Microsoft Windows 7 SP1 x64;
- Microsoft Windows 7 SP1 x64 для PT Industrial Cybersecurity Suite;

Примечание. В образ добавлены файлы-приманки, имитирующие ПО, характерное для узлов операторов SCADA-систем. Этот образ не включен в стандартную лицензию PT Email Security и приобретается отдельно.

- Microsoft Windows 8.1 Update 1 x64;
- Microsoft Windows 10 (1803) x64;
- Microsoft Windows 10 (1803) x64 с режимом загрузки UEFI;
- Microsoft Windows 10 (22H2) x64;
- Microsoft Windows 11 (23H2) x64;
- Microsoft Windows Server 2016 (1198) x64;
- Microsoft Windows Server 2019 (1879) x64.

Список установленного в образах дополнительного ПО указан в таблице. Если в таблице не указана версия ПО, установлена актуальная на момент создания образа версия.

Таблица 8. ПО, установленное в образах VM операционных систем семейства Windows

ПО	Windows				Windows Server	
	7 SP1 x64	8.1 x64	10	11	2016	2019
Adobe Acrobat Reader 2015	Да	Да	Да	Да	Да	Да
Adobe Flash Player 27	Да	Да	Да	Да	Да	Да
e2eSoft VCam 6.4	Да	Да	Да	Да	Да	Да
Google Chrome	—	—	Да	Да	Да	Да
Java Runtime Environment 8.0	Да	Да	Да	Да	Да	Да
Microsoft Access 2013	Да	Да	Да	—	Да	Да
Microsoft Access 2021	—	—	—	Да	—	—

ПО	Windows				Windows Server	
	7 SP1 x64	8.1 x64	10	11	2016	2019
Microsoft .NET Core Runtime 3.1	Да	Да	Да	Да	Да	Да
Microsoft .NET Framework 3.5	Да	Да	Да	Да	Да	Да
Microsoft .NET Framework 4.8	Да	Да	Да	Да	Да	Да
Microsoft Office 2013	Да	Да	Да	—	Да	Да
Microsoft Office 2021	—	—	—	Да	—	—
Microsoft Publisher 2013	Да	Да	Да	—	Да	Да
Microsoft Publisher 2021	—	—	—	Да	—	—
Microsoft Skype 7.39	Да	Да	Да	Да	Да	Да
Microsoft Visual C++ Redistributable for Visual Studio 2017 14.16	Да	Да	Да	Да	Да	Да
Microsoft Windows Subsystem for Linux (WSL) 2.0	—	—	Да	Да	Да	Да
Mozilla Firefox 67	Да	Да	Да	Да	Да	Да
Notepad++ 7.8	Да	Да	Да	Да	Да	Да
Opera	—	—	Да	Да	Да	Да
Opera 12.15	Да	Да	—	—	—	—
Piriform CCleaner	—	—	Да	Да	Да	Да
Piriform CCleaner 5.40	Да	Да	—	—	—	—
Python 3.8	Да	Да	Да	Да	Да	Да
Strawberry Perl	Да	Да	Да	Да	Да	Да
VideoLAN VLC media player 2.2	Да	Да	Да	Да	Да	Да
WinRAR 5.70	Да	Да	Да	Да	Да	Да

Образы ВМ операционных систем семейства Linux

В PT Email Security доступны образы ВМ со следующими версиями операционных систем семейства Linux:

- «Альт Рабочая станция» 10 x64;

Примечание. Этот образ не включен в стандартную лицензию PT Email Security и приобретается отдельно.

- «РЕД ОС» 7.3 «Муром» x64;

- «РЕД ОС» 8 x64;
- Astra Linux Special Edition 1.7 x64;
- Astra Linux Special Edition 1.8 x64;
- Ubuntu 22.04 LTS (Jammy Jellyfish) x64.

Список доступного в образах ПО указан в таблице. Это ПО может устанавливаться вместе со стандартными пакетами дистрибутива или отдельно. Если в таблице не указана версия ПО, установлена актуальная на момент создания образа версия.

Таблица 9. ПО, установленное в образах ВМ операционных систем семейства Linux

ПО	«Альт Рабочая станция» 10	«РЕД ОС»		Astra Linux SE		Ubuntu 22.04 LTS
		7.3 «Му- ром»	8	1.7	1.8	
Chromium	Да	Да	Да	Да	Да	Да
GNOME Desktop Environment	—	—	—	—	—	Да
KeePassXC	Да	Да	Да	Да	Да	Да
MATE Desktop Environment	Да	Да	Да	—	—	—
Microsoft .NET Framework 4	Да	Да	Да	—	—	Да
Mono	Да	Да	Да	Да	Да	Да
Mozilla Firefox	Да	Да	Да	Да	Да	Да
OpenJDK Java	Да	Да	Да	Да	Да	Да
Python	Да	Да	Да	Да	Да	Да
Samba	Да	Да	Да	Да	Да	Да
Wine	Да	Да	Да	Да	Да	Да

Приложение Г. Метки объектов

Метки устанавливаются при проверке объектов и отображаются в карточке объекта в блоке с его свойствами. Вы можете настроить фильтр объектов по меткам.

Таблица 10. Метки файлов

Метка	Описание
Архив	Файл является архивом
Зашифрованный	Доступ к содержимому файла ограничен паролем
Защищенный	Действия с файлом ограничены паролем (например, печать, копирование или изменение содержимого)
Использующие шаблон	Файл содержит ссылки на внешние шаблоны, определяющие форматирование и структуру документа
Многоотомный	Файл является частью многоотомного архива
Офисный	Файл офисного приложения Microsoft Office (Word, Excel, PowerPoint) и OpenDocument
Письмо	Файл является письмом
Поврежденный	Файл извлечен из архива или декодирован только частично, поскольку его размер превышает 512 MB
С OLE-объектами	Файл содержит объекты из других приложений, встроенные по технологии Object Linking and Embedding. Например, в документ могут быть встроены таблицы, диаграммы, формулы или рисунки
С запросами к внешним данным	Файл может автоматически извлекать данные из внешних источников, таких как базы данных, веб-сервисы или другие файлы
С макросами	В файле используются макросы, наборы инструкций или команд для автоматизации рутинных задач, обработки данных или интеграции с другими приложениями
С надстройками Office	В файле используются надстройки (add-ins) типа XLL или VSTO. Такие надстройки используются для добавления нестандартных инструментов, функций или автоматизации действий
С функциями DDE	В файле используется механизм Dynamic Data Exchange, позволяющий обмениваться данными и сообщениями с другими приложениями в реальном времени. Это позволяет, например, автоматически обновлять данные в документе, основываясь на изменениях в других приложениях

Метка	Описание
С элементами ActiveX	В файл встроены компоненты ActiveX для добавления нестандартных функций. Такие компоненты могут использоваться для внедрения интерактивных форм, элементов управления, медиаплееров или компонентов для обращения к внешним базам данных
Сжатый файл	Сжатый файл
Содержит Action	В файле настроены автоматические действия, запускаемые при выполнении пользователем определенных действий в документе, например при переходе по ссылке или нажатии на кнопку. Обычно это используется для выполнения сложных или повторяющихся задач
Содержит JavaScript	Файл содержит скрипты на языке JavaScript. Это могут быть сценарии для автоматизации задач, валидации форм, обработки событий и динамического изменения содержимого
Содержит OpenAction	В файле настроены автоматические действия, запускаемые при открытии документа. Обычно это используется для выполнения сложных или повторяющихся задач
Содержит PE-файл	Файл содержит вложенный исполняемый файл формата Portable Executable для Windows
Формат подделан	Файл имеет признаки изменения структуры или заголовков, которые не соответствуют его формату. Такие изменения могут использоваться злоумышленниками для сокрытия вредоносного содержимого или обхода статических методов проверки
ARCH AMD64	Файл для 64-битных операционных систем на архитектуре x86-64 (AMD64)
ARCH ARM	Файл для 32-битных операционных систем на архитектуре ARM
ARCH ARM64	Файл для 64-битных операционных систем на архитектуре ARM64 (ARMv8-A и новее)
ARCH I386	Файл для 32-битных операционных систем на архитектуре x86 (совместимой с Intel 80386)
SFX	Файл является самораспаковывающимся архивом
SFX 7z	Самораспаковывающийся архив формата 7z
SFX ACE	Самораспаковывающийся архив формата ACE
SFX RAR	Самораспаковывающийся архив формата RAR
SFX ZIP	Самораспаковывающийся архив формата ZIP

Метка	Описание
UPX	Файл сжат с помощью приложения UPX
ZIP-бомба	Файл является архивом, содержащим аномально большой объем данных. Распаковка такого архива может привести к исчерпанию дискового пространства и других системных ресурсов узла

Метки ссылок устанавливаются средством категоризации ссылок PT Categorizer в соответствии с тематикой ресурса, на который ведет ссылка.

Таблица 11. Метки ссылок

Метка	Описание
Academic Fraud	Сайты, предлагающие готовые работы, ответы к экзаменам и помощь в написании учебных материалов
Adult Sites	Сайты с материалами для взрослых, посвященные теме секса
Alcohol & Tobacco	Сайты с информацией об алкоголе и табаке, в том числе интернет-магазины алкогольной и табачной продукции
Anime	Сайты, посвященные аниме-культуре. Включают платформы для просмотра и обсуждения аниме-сериалов и фильмов
Arts	Сайты музеев и ресурсы, посвященные искусству
Astrology	Сайты, посвященные оккультизму и астрологии
Automotive	Сайты для автомобилистов, в том числе информационные порталы об автомобилях и ресурсы для покупки и продажи автомобилей, мотоциклов и других видов транспорта
Blogs	Блоги и персональные сайты, в том числе платформы для ведения онлайн-дневников и системы массового хостинга
Botnets & C2C	Ботнеты и командные центры для управления ими. Ботнеты — это ресурсы, контролируемые злоумышленниками удаленно. Используются для проведения кибератак, кражи данных, распространения вредоносного ПО и спама
Business	Сайты, посвященные бизнесу, маркетингу и экономике
Chats & Messengers	Сайты для обмена сообщениями, в том числе управляющие серверы приложений для обмена сообщениями
Classifieds	Доски объявлений — онлайн-платформы для публикации и поиска частных и коммерческих объявлений
Computers & Internet	Сайты, посвященные информационным технологиям, программному обеспечению, интернету и компьютерам

Метка	Описание
Corporate Sites	Корпоративные сайты организаций, представляющие компании, их продукты и услуги в интернете
Crypto Mining	Сайты, распространяющие программы для скрытого майнинга криптовалюты и использующие ресурсы устройств пользователей без их согласия. Такие сайты могут внедрять вредоносный код на устройства пользователей для майнинга криптовалюты
Dating	Сайты знакомств
DGA	Домены, созданные с помощью алгоритмов генерации доменных имен. Такие домены часто используются вредоносным ПО для уклонения от блокировки и обнаружения
Drugs	Сайты, рекламирующие или занимающиеся продажей наркотических веществ
E-commerce	Интернет-магазины
Education	Сайты образовательных учреждений и образовательные порталы
Entertainment	Сайты, посвященные досугу и развлечениям, в том числе ресурсы о кафе, ресторанах, кинотеатрах, концертных залах и других местах отдыха. Также сайты с информацией о предстоящих событиях, культурных мероприятиях, выставках и фестивалях
File Storage	Файловые хранилища и файлообменники — онлайн-сервисы, предоставляющие возможность загрузки, хранения и обмена файлами различных типов, включая документы, фотографии, видео и программное обеспечение
Finances	Сайты банков и других финансовых организаций, предоставляющие информацию о финансовых продуктах и услугах, в том числе о счетах, кредитах, вкладах, инвестициях и страховании
Forums	Форумы — онлайн-платформы для общения, на которых пользователи могут обсуждать различные темы, задавать вопросы и делиться мнениями
Gambling	Сайты, связанные с азартными играми, в том числе онлайн-казино, лотереи, ставки на спорт и тотализаторы
Games	Сайты, посвященные компьютерным и видеоиграм, в том числе платформы для игроков, новостные порталы об играх, обзоры, прохождения, советы и руководства
Generative AI	Платформы, предоставляющие инструменты и возможности для создания контента с использованием генеративного искусственного интеллекта

Метка	Описание
Government	Официальные сайты государственных органов
Hate & Discrimination	Сайты, которые были замечены в пропаганде агрессии, расизма и терроризма или распространении материалов, подстрекающих к ненависти, дискриминации и насилию на почве этнической принадлежности, религии, национальности или иных признаков
Health & Fitness	Сайты, посвященные здоровью и фитнесу, в том числе сайты больниц, поликлиник и других медицинских организаций, а также образовательные медицинские порталы
Home & Family	Сайты о домоводстве, семье и хобби
Humor	Юмористические и развлекательные сайты
Jobs & Career	Сайты для публикации резюме и вакансий, предназначенные для поиска работы и сотрудников
Justice Ministry's federal list	Материалы, внесенные Министерством Юстиции РФ в список экстремистских
Kids	Сайты для детей
Malware	Сайты, связанные с распространением вредоносного ПО, включая вирусы, трояны, шпионские и рекламные программы. Эти ресурсы могут заражать устройства пользователей, получать несанкционированный доступ к данным, шпионить за действиями или вмешиваться в работу систем
Movies & Video	Сайты для онлайн-просмотра фильмов и видео
Music & Radio	Музыкальные архивы и сайты онлайн-радиостанций
News & Media	Сайты новостных агентств и других средств массовой информации
Non-profit	Сайты некоммерческих организаций
Online Ads	Сайты рекламных и баннерных сетей, которые предназначены для размещения и управления онлайн-рекламой
Online Libraries	Онлайн-библиотеки, предоставляющие доступ к электронным книгам, аудиокнигам, научным работам и другим материалам
Paid sites of mobile operators	Сайты и сервисы, предоставляемые мобильными операторами на платной основе
Parked Domains	Запаркованные домены — это доменные имена, которые были зарегистрированы, но на данный момент не используются для ведения веб-сайта. Вместо этого на них размещается временная страница-заглушка, часто содержащая рекламу или информацию о том, что домен выставлен на продажу

Метка	Описание
Phishing & Typosquatting	Фишинговые сайты — мошеннические веб-ресурсы, созданные для обмана пользователей, кражи их личной информации (паролей, номеров кредитных карт, банковских данных) и других конфиденциальных сведений. Такие сайты могут маскироваться под легитимные страницы известных банков, платежных систем или социальных сетей, призывая пользователей ввести свои данные под различными предложениями, такими как необходимость верификации аккаунта или срочное обновление информации
Photo Sharing	Фотогалереи, архивы фотографий, фотостоки
Politics, Society and Law	Сайты, посвященные политике, обществу и законодательству, в том числе информационные порталы с политическими новостями, ресурсы политических партий и движений, а также справочники и базы данных законодательства
Pornography & Sexuality	Порнографические сайты
Portals	Объединение из нескольких сайтов одной тематики, предоставляющее пользователям доступ к разнообразной информации и сервисам в рамках единой платформы
Prosecutors orders	Сайты и материалы в сети, в отношении которых есть решение суда о запрете на публикацию
Ransomware	Сайты и ресурсы, связанные с распространением программ-вымогателей, которые блокируют доступ к данным или устройству и требуют выкуп за восстановление
Real Estate	Сайты с информацией о продаже и покупке недвижимости
Registry of banned sites	Сайты, заблокированные в соответствии с решением Роскомнадзора
Religious	Сайты религиозных и антирелигиозных организаций
Science & Technology	Сайты научных организаций и ресурсы, посвященные науке и технологиям
Search Engines	Поисковые системы
Shopping	Сайты о торговле и покупках, не относящиеся к категории интернет-магазинов
Social Networks	Социальные сети
Sports	Сайты, посвященные спорту или спортивным организациям
Tasteless	Сайты с избыточным количеством нецензурной лексики, грубостей или непристойностей, в том числе платформы и форумы, где отсутствует модерация и допускается использование грубой и оскорбительной речи

Метка	Описание
Torrents & P2P	Сайты торрент-трекеров и систем P2P (peer-to-peer). Предназначены для обмена файлами между пользователями в интернете без использования централизованного сервера
Trackers & Analytics	Системы трекинга для сбора данных о поведении пользователей в интернете и веб-аналитики
Travel	Сайты, посвященные туризму и путешествиям
VPN, Proxies & Anonymizers	VPN, прокси и анонимайзеры — это инструменты и сервисы, предоставляющие пользователям возможность обходить интернет-фильтры и ограничения, скрывая их истинный IP-адрес и обеспечивая анонимный доступ к веб-сайтам
Weapons	Сайты, посвященные армии или оружию
Webmail	Почтовые сайты, предоставляющие услуги электронной почты

Приложение Д. Синтаксис языка запросов QL

Язык запросов QL используется для поиска заданий на проверку и объектов заданий. Условие QL-запроса состоит из одного или нескольких предикатов, логических операторов и скобок (). Также QL-запрос может содержать оператор для сортировки результатов запроса.

Использовать QL-запросы вы можете на страницах **Задания**, **Объекты** и в карточке задания. Результатом поиска на странице **Объекты** и в карточке задания будут объекты, удовлетворяющие условию запроса. Результатом поиска на странице **Задания** будет список из заданий, которые удовлетворяют условию запроса, и заданий, в которых хотя бы один объект, удовлетворяет условию запроса.

Предикаты

Информация о заданиях и объектах сохраняется в PT Email Security в виде наборов полей. Каждое поле содержит информацию о некотором свойстве. Наборы полей различаются для заданий и объектов, но большинство полей общие, и вы можете использовать их для поиска как по свойствам заданий, так и по свойствам объектов.

Предикат — это логическое выражение вида <Поле> <Оператор> <Значение>. В предикате с помощью оператора объединяются поле задания или объекта и возможное значение этого поля. Указанное значение должно соответствовать типу данных поля. Если значение поля для сохраненного в PT Email Security задания или объекта соответствует указанным в предикате оператору и значению, то результатом будет True, иначе — False. Например, запрос с предикатом `age <= 1d` позволяет найти все задания, созданные за сутки, или все полученные за сутки объекты. Запрос с предикатом `correlated.verdict.threat.level = DANGEROUS` позволяет найти все опасные объекты или задания с такими объектами.

Примечание. Названия полей заданий и объектов чувствительны к регистру. Операторы для создания предикатов, логические операторы и оператор сортировки регистронезависимы.

Таблица 12. Операторы в предикатах QL-запроса

Оператор	Назначение	Синтаксис
=	Проверка на равенство	<Поле> = <Значение>
!=	Проверка на неравенство	<Поле> != <Значение>
>, <	Проверка на строгое неравенство. Только для типов данных DateTime и Integer (кроме отрицательных чисел)	<Поле> > <Значение> <Поле> < <Значение>
>=, <=	Проверка на нестрогое неравенство. Только для типов данных DateTime и Integer (кроме отрицательных чисел)	<Поле> >= <Значение> <Поле> <= <Значение>

Оператор	Назначение	Синтаксис
IN	Проверка на вхождение значения в список	<Поле> IN (<Значение 1>, ..., <Значение N>)
	Проверка на вхождение значения в диапазон. Только для типов данных DateTime и Integer (кроме отрицательных чисел)	<Поле> IN [<Значение 1>..<Значение N>]
NOT IN	Проверка на отсутствие значения в списке	<Поле> NOT IN (<Значение 1>, ..., <Значение N>)
	Проверка на отсутствие значения в диапазоне. Только для типов данных DateTime и Integer (кроме отрицательных чисел)	<Поле> NOT IN [<Значение 1>..<Значение N>]
LIKE	Проверка на неточное соответствие для одного поля. При проверке учитывается регистр. В шаблоне вы можете использовать символы % для любой последовательности символов и _ для одного любого символа	<Поле> LIKE <Шаблон>
ILIKE	Проверка на неточное соответствие для одного поля, независимо от регистра. В шаблоне вы можете использовать символы % для любой последовательности символов и _ для одного любого символа	<Поле> ILIKE <Шаблон>
~	Проверка на неточное соответствие для одного поля, независимо от регистра. В шаблоне вы можете использовать символы * для любой последовательности символов и ? для одного любого символа	<Поле> ~ <Шаблон>
text ~	Проверка на неточное соответствие для любых полей с типом данных String, независимо от регистра. В шаблоне вы можете использовать символы * — для любой последовательности символов и ? — для одного любого символа	text ~ <Шаблон>

Логические операторы и сортировка результатов

С помощью логических операторов AND, OR и NOT вы можете объединять в условии QL-запроса несколько предикатов, а с помощью скобок определять порядок их проверки. Например, запрос `age <= 1w AND (correlated.verdict.threat.level = DANGEROUS OR correlated.verdict.threat.level = UNWANTED)` позволяет найти все задания или все объекты с угрозами за неделю.

Таблица 13. Логические операторы в условии QL-запроса

Оператор	Назначение	Синтаксис
AND	Конъюнкция (логическое И)	<Предикат> AND <Предикат>
NOT	Отрицание (логическое НЕ)	NOT <Предикат>
OR	Дизъюнкция (логическое ИЛИ)	<Предикат> OR <Предикат>

Если необходимо настроить сортировку результатов запроса, после условия запроса укажите оператор `ORDER BY`, одно или несколько полей, по значениям которых будет выполняться сортировка, и способ сортировки. Например, запрос `age <= 1M AND correlated.verdict.threat.level = DANGEROUS ORDER BY start DESC` позволяет найти все опасные объекты или задания с такими объектами за месяц и отсортировать их по времени создания задания от новых к старым.

Таблица 14. Оператор ORDER BY для сортировки результатов QL-запроса

Назначение	Синтаксис
Сортировка по возрастанию	<Выражение> ORDER BY <Поле 1>, ..., <Поле N> ASC
Сортировка по убыванию	<Выражение> ORDER BY <Поле 1>, ..., <Поле N> DESC

Типы данных полей

В таблице указаны типы данных, которые используются для значений полей заданий и объектов.

Таблица 15. Типы данных

Тип	Назначение	Пример
Boolean	Логическое значение	True, False, 1, 0
DateTime	Дата в формате YYYY-MM-DD	2023-01-01
	Дата и время в формате YYYY-MM-DD HH:MM:SS или YYYY-MM-DDTHH:MM:SS	2023-01-01 10:00:00 2023-01-01T10:00:00
	Дата, время и часовой пояс в формате YYYY-MM-DDTHH:MM:SS+Z	2023-01-01T10:00:00+0300
Enum	Один из элементов предопределенного списка значений с типом данных String	COMPRESSED_FILE
Integer	Целое число	-3, 0, 12

Тип	Назначение	Пример
String	Строка. Значение нужно указывать в кавычках, но если значение не содержит специальных символов и пробелов, кавычки можно опустить	"archive.zip"

В этом разделе

[Поля QL-запросов \(см. приложение Д.1\)](#)

[Типы вредоносного ПО \(см. приложение Д.2\)](#)

Д.1. Поля QL-запросов

В таблице сгруппированы общие поля, которые вы можете использовать в QL-запросах для поиска заданий и объектов.

Таблица 16. Общие поля

Поле	Тип данных	Описание
age	Integer	Время существования задания в секундах. В запросах вы можете использовать единицы измерения: <i>m</i> — минута, <i>h</i> — час, <i>d</i> — день, <i>w</i> — неделя, <i>M</i> — месяц, <i>Y</i> — год
id, scan.id	String	Идентификатор задания
sandbox	Boolean	Проверен ли объект методом поведенческого анализа. Это поле можно использовать только для поиска объектов
start	DateTime	Время создания задания
start.date	DateTime	Дата создания задания
text	String	Специальное поле для поиска по значениям всех текстовых полей

Поля для свойств заданий

В таблице сгруппированы поля, которые вы можете использовать в QL-запросах для поиска только заданий по их свойствам или результатам проверки.

Таблица 17. Поля для свойств заданий

Поле	Тип данных	Описание
<code>action</code>	Enum	Решение о блокировке объекта: — BLOCK — заблокировать; — NOTHING — не требуется; — PASS — пропустить
<code>from_to</code>	String	Откуда и куда направлялся объект
<code>status</code>	Enum	Статус обработки задания: — FAIL — отказ; — SUCCESS — успех
<code>task.object.name</code>	String	Название задания
<code>task.object.type</code>	Enum	Тип объекта задания: — ARCHIVE — архив; — COMPRESSED_FILE — сжатый файл; — EMAIL — письмо; — EMAIL_BODY — тело письма; — FILE — файл; — FOLDER — папка; — HTTP — HTTP-сообщение; — SANDBOX_AMSI — AMSI-скрипт; — SANDBOX_DROP — dropped файл; — SANDBOX_MEMORY_DUMP — дамп памяти (memdump); — SANDBOX_PROCESS_MEMORY_DUMP — дамп памяти (procdump); — URL — ссылка
<code>task.processed_at</code>	DateTime	Дата и время решения о блокировке
<code>task.processed_elapsed</code>	Integer	Время от создания задания до решения о блокировке в секундах

Поле	Тип данных	Описание
<code>task.threat.weight</code>	Integer	Значение уровня опасности объекта задания от -1 до -200, по убыванию опасности. По модулю совпадает со значением <code>task.correlated.verdict.priority</code> . Используется для сортировки
<code>task.verdict_at</code>	DateTime	Дата и время вынесения вердикта по заданию
<code>task.verdict_elapsed</code>	Integer	Время от создания задания до вынесения вердикта в секундах
Результат проверки задания		
<code>task.correlated.state</code>	Enum	Статус проверки задания: — <code>FULL</code> — выполнена полностью; — <code>PARTIAL</code> — выполнена частично; — <code>UNSCANNED</code> — не выполнена
<code>task.correlated.verdict.priority</code>	Integer	Значение уровня опасности объекта задания. Три уровня по убыванию опасности для опасных объектов: 1–10, 11–40, 41–100. Три уровня для потенциально опасных: 101–115, 116–130, 131–199. Для безопасных — 200
<code>task.correlated.verdict.threat.classification</code>	Enum	Тип обнаруженного вредоносного ПО (см. приложение Д.2)
<code>task.correlated.verdict.threat.family</code>	String	Класс обнаруженного вредоносного ПО
<code>task.correlated.verdict.threat.level</code>	Enum	Уровень опасности объекта: — <code>CLEAN</code> — без обнаруженных угроз; — <code>DANGEROUS</code> — опасный; — <code>UNWANTED</code> — потенциально опасный
<code>task.correlated.verdict.threat.platform</code>	Enum	Операционная система обнаруженного вредоносного ПО: — <code>ANDROID</code>; — <code>IOS</code>; — <code>LINUX</code>; — <code>NO_PLATFORM</code>;

Поле	Тип данных	Описание
		— OSX; — WINDOWS
Результат проверки задания методом поведенческого анализа		
<code>task.sandbox.correlated.state</code>	Enum	Статус поведенческого анализа: — FULL — выполнена полностью; — PARTIAL — выполнена частично; — UNSCANNED — не выполнена
<code>task.sandbox.correlated.verdict.priority</code>	Integer	Значение уровня опасности объекта, согласно поведенческому анализу. Три уровня по убыванию опасности для опасных объектов: 1–10, 11–40, 41–100. Три уровня для потенциально опасных: 101–115, 116–130, 131–199. Для безопасных — 200
<code>task.sandbox.correlated.verdict.threat.classification</code>	Enum	Тип обнаруженного вредоносного ПО (см. приложение Д.2)
<code>task.sandbox.correlated.verdict.threat.family</code>	String	Класс обнаруженного вредоносного ПО
<code>task.sandbox.correlated.verdict.threat.level</code>	Enum	Уровень опасности объекта: — CLEAN — без обнаруженных угроз; — DANGEROUS — опасный; — UNWANTED — потенциально опасный
<code>task.sandbox.correlated.verdict.threat.platform</code>	Enum	Операционная система обнаруженного вредоносного ПО: — ANDROID; — IOS; — LINUX; — NO_PLATFORM; — OSX; — WINDOWS
<code>task.sandbox.is_in_progress</code>	Boolean	Выполняется ли поведенческий анализ в настоящий момент

Поля с результатами проверки объекта

В таблице сгруппированы поля, которые вы можете использовать в QL-запросах для поиска заданий и объектов по результатам проверки объектов.

Таблица 18. Поля с результатами проверки объекта

Поле	Тип данных	Описание
<code>av.any.detections.name</code>	String	Название вредоносного ПО, обнаруженного любым антивирусом
<code>av.any.detections.threat.classification</code>	Enum	Тип вредоносного ПО, обнаруженного любым антивирусом (см. приложение Д.2)
<code>bw_lists.errors.type</code>	Enum	Тип ошибки при проверке по черному и белому спискам: — <code>COLLISION_ERROR</code>; — <code>ENGINE_ERROR</code>; — <code>LISTS_NOT_READY_ERROR</code>; — <code>SCAN_MACHINE_ERROR</code>; — <code>TIMEOUT_ERROR</code>
<code>bw_lists.hashes</code>	Enum	Тип хеш-суммы объекта из черного или белого списка: — <code>MD5</code>; — <code>SHA1</code>; — <code>SHA256</code>
<code>bw_lists.state</code>	Enum	Статус проверки по черному и белому спискам: — <code>FULL</code> — выполнена полностью; — <code>PARTIAL</code> — выполнена частично; — <code>UNSCANNED</code> — не выполнена
<code>bw_lists.status</code>	Enum	Результат проверки по черному и белому спискам: — <code>IN_BLACK_LIST</code> — в черном списке; — <code>IN_WHITE_LIST</code> — в белом списке; — <code>NOT_IN_LISTS</code> — отсутствует в списках

Поле	Тип данных	Описание
<code>correlated.state</code>	Enum	Статус проверки объекта: — <code>FULL</code> — выполнена полностью; — <code>PARTIAL</code> — выполнена частично; — <code>UNSCANNED</code> — не выполнена
<code>correlated.threat_source</code>	Boolean	Является ли объект причиной вердикта или наследует его от дочернего
<code>correlated.verdict.priority</code>	Integer	Значение уровня опасности объекта. Три уровня по убыванию опасности для опасных объектов: 1–10, 11–40, 41–100. Три уровня для потенциально опасных: 101–115, 116–130, 131–199. Для безопасных — 200
<code>correlated.verdict.threat.classification</code>	Enum	Тип вредоносного ПО согласно вердикту по объекту (см. приложение Д.2)
<code>correlated.verdict.threat.family</code>	String	Класс вредоносного ПО объекта
<code>correlated.verdict.threat.level</code>	Enum	Уровень опасности объекта: — <code>CLEAN</code> — без обнаруженных угроз; — <code>DANGEROUS</code> — опасный; — <code>UNWANTED</code> — потенциально опасный
<code>correlated.verdict.threat.platform</code>	Enum	Операционная система вредоносного ПО объекта: — <code>ANDROID</code>; — <code>IOS</code>; — <code>LINUX</code>; — <code>NO_PLATFORM</code>; — <code>OSX</code>; — <code>WINDOWS</code>
<code>detections.name</code>	String	Название вредоносного ПО, обнаруженного любым средством проверки
<code>detections.threat.classification</code>	Enum	Тип вредоносного ПО, обнаруженного любым средством проверки (см. приложение Д.2)

Поле	Тип данных	Описание
threat.weight	Integer	Значение уровня опасности объекта от -1 до -200, по убыванию опасности. По модулю совпадает со значением <code>correlated.verdict.priority</code> . Используется для сортировки
Результат проверки ссылки средством категоризации		
ptcategorizer.categories	String	Установленные категории ссылок
ptcategorizer.database.time	DateTime	Дата и время обновления базы знаний
ptcategorizer.database.version	String	Версия базы знаний
ptcategorizer.errors.type	Enum	Тип ошибки, возникшей при проверке: — ANALYSIS_ERROR; — CONTAINS_CORRUPTED; — CONTAINS_ENCRYPTED; — CORRUPTED; — ENCRYPTED; — ENGINE_ERROR; — FILE_NOT_FOUND; — LIMIT_EXCEEDED; — SCAN_MACHINE_ERROR; — TIMEOUT_ERROR; — UNPACKING_ERROR
ptcategorizer.state	Enum	Статус проверки: — FULL — выполнена полностью; — PARTIAL — выполнена частично; — UNSCANNED — не выполнена
ptcategorizer.version	String	Версия PT Categorizer

Поле	Тип данных	Описание
Результат проверки объекта определенным средством проверки		
В префиксе полей вы можете указывать следующие средства проверки:		
— <code>antiphishing</code> — средство для защиты от угроз в почте PT Anti-Phishing and Anti-Spam; — <code>av.avast</code> — антивирус Avast Core Security; — <code>av.clamav</code> — антивирус ClamAV; — <code>av.kaspersky</code> — антивирус Kaspersky Web Traffic Security; — <code>av.ptav</code> — антивирус PT AV; — <code>av.vba</code> — антивирус VBA32; — <code>ptes</code> — средство статического анализа на основе YARA-правил PT ESC; — <code>ptioc</code> — средство обнаружения индикаторов компрометации PT IoC; — <code>rule_engine</code> — пользовательские правила определения объектов с угрозами; — <code>sandbox.network</code> — средство поведенческого анализа сетевых пакетов PT DPI; — <code>yara_engine</code> — средство проверки по пользовательским YARA-правилам (действующие правила); — <code>yara_engine_test</code> — средство проверки по пользовательским YARA-правилам (тестовые правила)		
<code><Средство проверки>.database.time</code>	DateTime	Дата и время обновления базы знаний
<code><Средство проверки>.database.version</code>	String	Версия базы знаний
<code><Средство проверки>.detections.description</code>	String	Описание обнаруженной угрозы (доступно только для средства проверки PT DPI)
<code><Средство проверки>.detections.id</code>	String	Идентификатор обнаруженной угрозы (доступно только для средства проверки PT DPI)
<code><Средство проверки>.detections.is_apt</code>	Boolean	Обнаружены ли признаки целевой атаки
<code><Средство проверки>.detections.is_exact</code>	Boolean	Является ли обнаружение точным
<code><Средство проверки>.detections.name</code>	String	Название обнаруженного вредоносного ПО

Поле	Тип данных	Описание
<code><Средство проверки>.detections.threat.classification</code>	Enum	Тип обнаруженного вредоносного ПО (см. приложение Д.2)
<code><Средство проверки>.detections.threat.family</code>	String	Класс обнаруженного вредоносного ПО
<code><Средство проверки>.detections.threat.platform</code>	Enum	Операционная система обнаруженного вредоносного ПО: — ANDROID; — IOS; — LINUX; — NO_PLATFORM; — OSX; — WINDOWS
<code><Средство проверки>.errors.type</code>	Enum	Тип ошибки, возникшей при проверке: — ANALYSIS_ERROR; — CONTAINS_CORRUPTED; — CONTAINS_ENCRYPTED; — CORRUPTED; — ENCRYPTED; — ENGINE_ERROR; — FILE_NOT_FOUND; — LIMIT_EXCEEDED; — SCAN_MACHINE_ERROR; — TIMEOUT_ERROR; — UNPACKING_ERROR
<code><Средство проверки>.state</code>	Enum	Статус проверки: — FULL — выполнена полностью; — PARTIAL — выполнена частично; — UNSCANNED — не выполнена

Поле	Тип данных	Описание
<code><Средство проверки>.verdict.threat.classification</code>	Enum	Тип вредоносного ПО согласно вердикту средства проверки (см. приложение Д.2)
<code><Средство проверки>.verdict.threat.family</code>	String	Класс вредоносного ПО согласно вердикту средства проверки
<code><Средство проверки>.verdict.threat.level</code>	Enum	Уровень опасности объекта согласно вердикту средства проверки: — CLEAN — без обнаруженных угроз; — DANGEROUS — опасный; — UNWANTED — потенциально опасный
<code><Средство проверки>.verdict.threat.platform</code>	Enum	Операционная система вредоносного ПО согласно вердикту средства проверки: — ANDROID; — IOS; — LINUX; — NO_PLATFORM; — OSX; — WINDOWS
<code><Средство проверки>.version</code>	String	Версия средства проверки

Поля для свойств поведенческого анализа объектов

В таблице сгруппированы поля, которые вы можете использовать в QL-запросах для поиска заданий и объектов по свойствам и результатам поведенческого анализа объектов.

Таблица 19. Поля для свойства поведенческого анализа объектов

Поле	Тип данных	Описание
<code>sandbox.bootkitmon</code>	Boolean	Выполнялась ли перезагрузка ОС при поведенческом анализе

Поле	Тип данных	Описание
sandbox.bootkitmon_stage	Enum	Этап поведенческого анализа относительно перезагрузки ОС: — AFTER_REBOOT; — BEFORE_REBOOT
sandbox.duration	Integer	Общая продолжительность поведенческого анализа в секундах
sandbox.errors.type	Enum	Тип ошибки, возникшей при поведенческом анализе: — ENGINE_ERROR; — FILE_NOT_FOUND; — INIT_ERROR; — NOT_ENOUGH_IMAGE_COPIES; — SCAN_MACHINE_ERROR; — TIMEOUT_ERROR; — UNKNOWN
sandbox.file_type	String	Тип файла, отправленного на поведенческий анализ
sandbox.image.name	String	Название образа VM
sandbox.image.os.architecture	String	Архитектура ОС образа VM
sandbox.image.os.locale	String	Язык ОС образа VM
sandbox.image.os.name	String	Название ОС образа VM
sandbox.image.os.service_pack	String	Версия пакета обновлений ОС образа VM
sandbox.image.os.version	String	Версия ОС образа VM
sandbox.image.version	String	Версия образа VM
sandbox.init_msdn_error.code	Integer	Код ошибки MSDN при запуске поведенческого анализа
sandbox.init_msdn_error.name	String	Название ошибки MSDN при запуске поведенческого анализа
sandbox.item.process.name	String	Имя процесса при поведенческом анализе
sandbox.item.trigger	String	Причина снятия дампа памяти процесса при поведенческом анализе

Поле	Тип данных	Описание
sandbox.mitm	Boolean	Выполнялась ли расшифровка HTTPS-трафика при поведенческом анализе
sandbox.planned_duration	Integer	Планируемая продолжительность поведенческого анализа в секундах
sandbox.produced	Boolean	Является ли объект артефактом поведенческого анализа
sandbox.rules_version.correlation	String	Версия правил корреляции для поведенческого анализа
sandbox.rules_version.dpi	String	Версия правил анализа сетевых пакетов для поведенческого анализа
sandbox.state	Enum	Статус поведенческого анализа: — FULL — выполнен полностью; — PARTIAL — выполнен частично; — UNSCANNED — не выполнен
Результат поведенческого анализа объекта		
sandbox.behaviors.mitre_threat_id	String	Идентификатор подозрительного поведения объекта согласно базе знаний MITRE ATT&CK
sandbox.behaviors.name	String	Название подозрительного поведения объекта
sandbox.behaviors.weight	Integer	Степень опасности подозрительного поведения объекта
sandbox.detections.name	String	Название обнаруженного вредоносного ПО
sandbox.detections.threat_classification	Enum	Тип обнаруженного вредоносного ПО (см. приложение Д.2)
sandbox.detections.threat_family	String	Класс обнаруженного вредоносного ПО
sandbox.detections.threat_platform	Enum	Операционная система обнаруженного вредоносного ПО: — ANDROID; — IOS; — LINUX; — NO_PLATFORM;

Поле	Тип данных	Описание
		— OSX; — WINDOWS
<code>sandbox.network.behaviors.description</code>	String	Описание атаки, выявленной средством анализа сетевых пакетов
<code>sandbox.network.behaviors.id</code>	String	Идентификатор атаки, выявленной средством анализа сетевых пакетов
<code>sandbox.network.behaviors.name</code>	String	Название атаки, выявленной средством анализа сетевых пакетов
<code>sandbox.verdict.threat.classification</code>	Enum	Тип обнаруженного вредоносного ПО (см. приложение Д.2)
<code>sandbox.verdict.threat.family</code>	String	Класс обнаруженного вредоносного ПО
<code>sandbox.verdict.threat.level</code>	Enum	Уровень опасности объекта: — CLEAN — без обнаруженных угроз; — DANGEROUS — опасный; — UNWANTED — потенциально опасный
<code>sandbox.verdict.threat.platform</code>	Enum	Операционная система обнаруженного вредоносного ПО: — ANDROID; — IOS; — LINUX; — NO_PLATFORM; — OSX; — WINDOWS
Результат по всем артефактам поведенческого анализа		
<code>sandbox.correlated.state</code>	Enum	Статус поведенческого анализа: — FULL — выполнен полностью; — PARTIAL — выполнен частично; — UNSCANNED — не выполнен
<code>sandbox.correlated.verdict.threat.classification</code>	Enum	Тип обнаруженного вредоносного ПО (см. приложение Д.2)

Поле	Тип данных	Описание
<code>sandbox.correlated.verdict.threat.family</code>	String	Класс обнаруженного вредоносного ПО
<code>sandbox.correlated.verdict.threat.level</code>	Enum	Уровень опасности объекта: — CLEAN — без обнаруженных угроз; — DANGEROUS — опасный; — UNWANTED — потенциально опасный
<code>sandbox.correlated.verdict.threat.platform</code>	Enum	Операционная система обнаруженного вредоносного ПО: — ANDROID; — IOS; — LINUX; — NO_PLATFORM; — OSX; — WINDOWS

Поля для свойств объектов

В таблице сгруппированы поля, которые вы можете использовать в QL-запросах для поиска заданий и объектов по свойствам объектов.

Таблица 20. Поля для свойств объектов

Поле	Тип данных	Описание
<code>ancestor.node_id</code>	Integer	Идентификатор дочернего объекта в карточке задания. Это поле можно использовать только для поиска объектов
<code>errors.type</code>	Enum	Тип ошибки, возникшей при проверке: — ANALYSIS_ERROR; — CONNECT_TIMEOUT; — CONTAINS_CORRUPTED; — CONTAINS_ENCRYPTED; — CORRUPTED; — ENCRYPTED;

Поле	Тип данных	Описание
		— ENGINE_ERROR; — FILE_NOT_FOUND; — INIT_ERROR; — LIMIT_EXCEEDED; — MAX_REDIRECT_EXCEEDED; — MAX_SIZE_EXCEEDED; — NOT_ENOUGH_IMAGE_COPIES; — NOT_FILE; — NO_SUITABLE_UNPACKER; — READ_TIMEOUT; — SCAN_MACHINE_ERROR; — TIMEOUT_ERROR; — UNKNOWN; — UNPACKING_ERROR
network_objects.any	String	Значение для поиска по любым сетевым объектам
network_objects.url	String	Значение для поиска ссылок среди сетевых объектов
node.type	Enum	Тип элемента в карточке задания: — ARTIFACT — карточка объекта; — SANDBOX — карточка поведенческого анализа; — SANDBOX_STAGE — карточка поведенческого анализа с перезагрузкой
object.file_extension	String	Расширение файла
object.file_group	Enum	Группа типов файлов: — data-files/ — файлы данных; — data-files/archives-and-compressed/ — архивы и сжатые файлы; — data-files/disk-images/ — образы дисков;

Поле	Тип данных	Описание
		— <code>data-files/network-traffic-dumps/</code> — дампы сетевого трафика; — <code>data-files/tabular-data-formats/</code> — табличные данные; — <code>data-files/text-data/</code> — текстовые данные; — <code>executable-files/</code> — исполняемые файлы; — <code>executable-files/cross-platform-scripts/</code> — мультиплатформенные скрипты; — <code>executable-files/distributions/</code> — установочные пакеты; — <code>executable-files/html-documents/</code> — документы HTML; — <code>executable-files/java/</code> — Java; — <code>executable-files/linux-based/</code> — для семейства Linux; — <code>executable-files/windows/</code> — для Windows; — <code>images/</code> — графические файлы; — <code>images/raster/</code> — растровые; — <code>office-applications/</code> — файлы офисных приложений; — <code>office-applications/documents/</code> — документы; — <code>office-applications/post/</code> — письма; — <code>office-applications/presentations/</code> — презентации; — <code>office-applications/tables/</code> — таблицы; — <code>other/</code> — другие файлы; — <code>specialized-applications/</code> — файлы приложений;

Поле	Тип данных	Описание
		— <code>specialized-applications/databases/</code> — базы данных; — <code>system-files/</code> — системные файлы; — <code>system-files/libraries-drivers/</code> — библиотеки и драйверы; — <code>system-files/others/</code> — другие системные файлы
<code>object.file_type</code>	String	Тип файла, определенный PT ESC
<code>object.from_cache</code>	Boolean	Получен ли объект из кэша
<code>object.magic_string</code>	String	Дополнительная информация об объекте
<code>object.md5</code>	String	Хеш-сумма MD5 объекта
<code>object.mime_type</code>	String	MIME-тип объекта
<code>object.name</code>	String	Название объекта
<code>object.properties</code>	Enum	Метки объекта: — <code>ARCHIVE</code> — архив; — <code>COMPRESSED</code> — сжатый файл; — <code>EMAIL</code> — письмо; — <code>ENCRYPTED</code> — зашифрованный; — <code>HAS_ACTION</code> — содержит Action; — <code>HAS_ACTIVE_X</code> — с элементами ActiveX; — <code>HAS_ADD_IN</code> — с надстройками Office; — <code>HAS_DDE</code> — с функциями DDE; — <code>HAS_EMBEDDED</code> — с OLE-объектами; — <code>HAS_JAVASCRIPT</code> — содержит JavaScript; — <code>HAS_MACROS</code> — с макросами; — <code>HAS_OPEN_ACTION</code> — содержит OpenAction; — <code>HAS_REMOTE_DATA</code> — с запросами к внешним данным; — <code>HAS_REMOTE_TEMPLATE</code> — использует внешний шаблон; — <code>MULTI_VOLUME</code> — многотомный архив;

Поле	Тип данных	Описание
		— OFFICE — файл офисного формата; — SFX — самораспаковывающийся архив; — SFX_7z — самораспаковывающийся архив формата 7z; — SFX_ACE — самораспаковывающийся архив формата ACE; — SFX_RAR — самораспаковывающийся архив формата RAR; — SFX_ZIP — самораспаковывающийся архив формата ZIP; — UPX — файл сжат с помощью приложения UPX
object.sha1	String	Хеш-сумма SHA-1 объекта
object.sha256	String	Хеш-сумма SHA-256 объекта
object.size	Integer	Размер объекта в байтах. В запросах вы можете использовать единицы измерения KB, MB, GB, TB, PB
object.ssdeep	String	Хеш-сумма SSDEEP объекта
object.type	Enum	Тип объекта: — ARCHIVE — архив; — COMPRESSED_FILE — сжатый файл; — EMAIL — письмо; — EMAIL_BODY — тело письма; — FOLDER — папка; — FILE — файл; — HTTP — HTTP-сообщение; — SANDBOX_AMSI — AMSI-скрипт; — SANDBOX_DROP — dropped файл; — SANDBOX_MEMORY_DUMP — дамп памяти (memdump);

Поле	Тип данных	Описание
		— <code>SANDBOX_PROCESS_MEMORY_DUMP</code> — дамп памяти (procdump); — <code>URL</code> — ссылка
<code>parent.node_id</code>	Integer	Идентификатор родительского объекта в карточке задания. Это поле можно использовать только для поиска объектов
<code>source.object.name</code> (<code>parent_object.name</code>)	String	Название родительского объекта
<code>source.object.type</code> (<code>parent_object.type</code>)	Enum	Тип родительского объекта: — <code>ARCHIVE</code> — архив; — <code>COMPRESSED_FILE</code> — сжатый файл; — <code>EMAIL</code> — письмо; — <code>EMAIL_BODY</code> — тело письма; — <code>FILE</code> — файл; — <code>HTTP</code> — HTTP-сообщение; — <code>SANDBOX_AMSI</code> — AMSI-скрипт; — <code>SANDBOX_DROP</code> — dropped файл; — <code>SANDBOX_MEMORY_DUMP</code> — дамп памяти (memdump); — <code>SANDBOX_PROCESS_MEMORY_DUMP</code> — дамп памяти (procdump); — <code>URL</code> — ссылка
<code>unpacker.errors.type</code>	Enum	Тип ошибки при извлечении дочерних объектов: — <code>CORRUPTED</code>; — <code>ENCRYPTED</code>; — <code>ENGINE_ERROR</code>; — <code>FILE_NOT_FOUND</code>; — <code>LIMIT_EXCEEDED</code>; — <code>NO_SUITABLE_UNPACKER</code>; — <code>SCAN_MACHINE_ERROR</code>;

Поле	Тип данных	Описание
		— TIMEOUT_ERROR; — UNKNOWN
unpacker.state	Enum	Статус извлечения дочерних объектов: — FULL — выполнено полностью; — PARTIAL — выполнено частично; — UNSCANNED — не выполнено

Свойства письма

email.bcc.address	String	Адрес получателя скрытой копии письма
email.bcc.name	String	Имя получателя скрытой копии письма
email.cc.address	String	Адрес получателя копии письма
email.cc.name	String	Имя получателя копии письма
email.from.address	String	Адрес отправителя письма
email.from.name	String	Имя отправителя письма
email.headers.name	String	Название заголовка для поиска по письмам
email.headers.value	String	Значение заголовка для поиска по письмам
email.id	String	Идентификатор письма
email.subject	String	Тема письма
email.to.address	String	Адрес получателя письма
email.to.name	String	Имя получателя письма
envelope.from	String	Адрес отправителя в заголовке письма
envelope.recipients	String	Адреса получателей в заголовке письма
envelope.result.action	Enum	Решение о блокировке письма: — BLOCK — заблокировать; — NOTHING — не требуется; — PASS — пропустить
envelope.result.delivery_status	Enum	Статус доставки проверенного письма: — FAIL — не доставлено; — SKIP — неизвестен; — SUCCESS — доставлено

Поле	Тип данных	Описание
<code>envelope.result.email_type</code>	Enum	Что доставлено получателям письма: — <code>DISARMED</code> — обезвреженное письмо; — <code>NOTHING</code> — ничего; — <code>NOTIFICATION</code> — уведомление; — <code>SOURCE</code> — исходное письмо
<code>envelope.result.recipient</code>	String	Адрес получателя в заголовке письма
<code>envelope.result.smtp_address</code>	String	Адрес SMTP-сервера, который использовался для доставки проверенного письма
<code>quarantine.event.recipient</code>	String	Адрес получателя письма из карантина
<code>quarantine.event.type</code>	Enum	Тип события в истории карантина: — <code>COMMENT</code> — добавлен комментарий; — <code>FORWARD</code> — переадресовано; — <code>MANUAL_DELETE</code> — вручную удалено; — <code>PROCESS</code> — изменена информация; — <code>QUARANTINE</code> — помещено в карантин; — <code>RELEASE</code> — выпущено; — <code>REMOVE</code> — удалено из карантина; — <code>SEND</code> — отправлена копия
<code>quarantine.sends_count</code>	Integer	Общее количество отправок письма из карантина
<code>quarantine.state</code>	Enum	Действие, выполненное с заблокированным письмом: — <code>QUARANTINED</code> — помещено в карантин; — <code>REMOVED</code> — удалено
Свойства ссылки		
<code>download_url.engine_version</code>	String	Версия средства для скачивания контента по ссылкам

Поле	Тип данных	Описание
<code>download_url.errors.type</code>	Enum	Тип ошибки, возникшей при скачивании контента по ссылке: — <code>CONNECT_TIMEOUT</code>; — <code>ENGINE_ERROR</code>; — <code>FILE_NOT_FOUND</code>; — <code>MAX_REDIRECT_EXCEEDED</code>; — <code>MAX_SIZE_EXCEEDED</code>; — <code>NOT_FILE</code>; — <code>READ_TIMEOUT</code>; — <code>SCAN_MACHINE_ERROR</code>; — <code>TIMEOUT_ERROR</code>; — <code>UNKNOWN</code>
<code>download_url.reason_phrase</code>	String	Статус ответа на HTTP-запрос по ссылке
<code>download_url.state</code>	Enum	Статус проверки ссылки: — <code>FULL</code> — выполнена полностью; — <code>PARTIAL</code> — выполнена частично; — <code>UNSCANNED</code> — не выполнена
<code>download_url.status_code</code>	Integer	Код ответа на HTTP-запрос по ссылке
<code>source.crawler.engine_name</code>	Enum	Тип средства для скачивания контента по ссылкам: — <code>CURL</code>; — <code>WEB_ENGINE</code>
<code>source.crawler.url</code>	String	Ссылка, по которой скачан файл
<code>url</code>	String	Ссылка, поступившая на проверку
<code>url.domain</code>	String	Домен второго уровня в ссылке
<code>url.subdomain</code>	String	Домен третьего уровня в ссылке
<code>url.redirects.status</code>	Integer	Код ответа на HTTP-запрос при перенаправлении
<code>url.redirects.url</code>	String	Ссылка при перенаправлении

Поле	Тип данных	Описание
Свойства HTTP-сообщения		
http.direction	Enum	Направление HTTP-вызова: — REQUEST; — RESPONSE
http.request.content_type	String	Тип содержимого в HTTP-запросе (Content-Type)
http.request.host	String	Адрес узла, которому направлен HTTP-запрос (Host)
http.request.method	String	Метод HTTP-запроса
http.request.referer	String	Ссылка на предыдущую страницу в HTTP-запросе (Referer)
http.request.url	String	URL-адрес в HTTP-запросе
http.request.user_agent	String	Информация о клиенте в HTTP-запросе (User-Agent)
http.request.x_forwarded_for	String	Адрес первого клиента в HTTP-запросе (X-Forwarded-For)
http.response.code	Integer	Код HTTP-ответа
http.response.content_disposition	String	Способ обработки HTTP-ответа (Content-Disposition)
http.response.content_type	String	Тип содержимого в HTTP-ответе (Content-Type)
http.response.reason	String	Статус HTTP-ответа
http.response.server	String	Адрес узла, сформировавшего HTTP-ответ

Поля для свойств источников

В таблице сгруппированы поля, которые вы можете использовать в QL-запросах для поиска заданий и объектов по свойствам источников объектов.

Таблица 21. Свойства источников

Поле	Тип данных	Описание
entry_point.id	String	Идентификатор источника
entry_point.name	String	Название источника

Поле	Тип данных	Описание
entry_point.type	Enum	Тип источника: — CHECK_ME — служба Checkme; — FILE_INBOX — папка-шлюз; — FILE_MONITOR — общая папка; — ICAP — ICAP-сервер; — INTERACTIVE_ANALYSIS — веб-интерфейс (ручной поведенческий анализ); — MAIL_AGENT — сервер Microsoft Exchange с установленным агентом; — MAIL_AGENT_MTA — почтовый шлюз безопасности; — MAIL_BCC — почтовый сервер в режиме зеркалирования; — MAIL_GATEWAY — почтовый сервер в режиме фильтрации; — MAIL_GATEWAY_MTA — почтовый сервер в режиме фильтрации (MTA); — PT_EDR — MaxPatrol EDR; — PTNAD — PT NAD; — PUBLIC_API — API с передаваемыми параметрами проверки; — RETRO — хранилище файлов (ретроспективный анализ); — SCAN_API — API с выбранными параметрами проверки; — WEB — веб-интерфейс
entry_point.metadata.name	String	Название поля для поиска по метаданным источника
entry_point.metadata.value	String	Значение поля для поиска по метаданным источника
file_inbox.dst	String	Имя папки после проверки
file_inbox.src	String	Имя папки до проверки
file_monitor.src	String	Имя общей папки

Поле	Тип данных	Описание
web.referer	String	Ссылка на страницу в HTTP-запросе на проверку объекта (Referer)
web.user_agent	String	Информация о клиенте в HTTP-запросе на проверку объекта (User-Agent)
web.x_forwarded_for	String	Адрес первого клиента в HTTP-запросе на проверку объекта (X-Forwarded-For)
Веб-интерфейс		
user.id	String	Идентификатор пользователя
user.is_anonymous	Boolean	Является ли пользователь анонимным
user.login	String	Логин пользователя
user.name	String	Имя пользователя
ICAP-сервер		
icap.client.ip	String	IP-адрес ICAP-клиента
icap.client.username	String	Имя пользователя ICAP-клиента
icap.method	String	Метод ICAP
icap.url	String	URL-адрес ICAP-сервера
icap.version	String	Версия ICAP
PT NAD		
ptnad.dst.ip	String	IP-адрес узла — получателя пакета
ptnad.dst.port	Integer	Порт узла — получателя пакета
ptnad.http.host	String	Имя узла-получателя (Host)
ptnad.http.referer	String	Ссылка на предыдущую страницу (Referer)
ptnad.http.uri	String	URI запрашиваемой страницы
ptnad.http.user_agent	String	Информация о клиенте (User-Agent)
ptnad.proto	String	Сетевой протокол
ptnad.src.ip	String	IP-адрес узла — отправителя пакета
ptnad.src.port	Integer	Порт узла — отправителя пакета

Д.2. Типы вредоносного ПО

В таблице указаны возможные значения полей для поиска по типам вредоносного ПО.

Таблица 22. Типы вредоносного ПО

Значение	Тип	Описание
ADWARE	Рекламное ПО	Программное обеспечение, распространяемое в рекламных целях. Незаметно попав на устройство, оно демонстрирует пользователю рекламу, а также собирает пользовательскую информацию для партнерских программ. Может вводить владельца устройства в заблуждение для легитимизации своего присутствия
BACKDOOR	Бэкдор	Вредоносное ПО для скрытого удаленного управления устройством. Представители этого класса — неотъемлемая часть целевых атак
BOOTKIT	Буткит	Вредоносное ПО, запускающее вредоносный код на самых ранних этапах загрузки ОС
CLIENT_IRC	IRC-клиент	Программа, используемая для коммуникации в IRC (Internet Relay Chat), обмена файлами и управляющими командами с применением нестандартного протокола связи. Не является вредоносной, но может быть использована злоумышленниками
CLIENT_P2P	P2P-клиент	Программа, используемая для работы с peer-to-peer-сетями. Применяется для обмена информацией в распределенной архитектуре хранения и передачи данных. Не является вредоносной, но может быть использована злоумышленниками
CLIENT_SMTP	SMTP-клиент	Программа, используемая для отправки электронных писем в скрытом режиме. Чаще применяется в составе многофункционального ПО. Не является вредоносной, но может быть использована злоумышленниками
CONSTRUCTOR	Конструктор	Программа для сборки новых образцов вредоносного ПО. Злоумышленники используют ее при подготовке к атаке. Продается на теневых форумах
DIALER	Средство дозвона	Программа, используемая для установки телефонных соединений в скрытом режиме. Не является вредоносной, но может быть использована злоумышленниками
DOS	DoS-утилита	Программа для проведения атаки типа «отказ в обслуживании». При отправке большого числа запросов принимающая сторона не успевает их обработать и становится временно недоступной. Может использоваться для вывода из строя средств защиты

Значение	Тип	Описание
DOWNLOADER	Загрузчик	Программа для скрытого скачивания данных из сетевых источников. Чаще применяется в составе многофункционального ПО. Не является вредоносной, но может быть использована злоумышленниками
EMAIL_FLOODER	Почтовый спамер	Программа для отправки большого количества бесполезной информации с помощью электронной почты. Может быть использована для рассылки спама, отвлечения внимания пользователя или обхода средств защиты
EMAIL_WORM	Почтовый червь	Вредоносное ПО, способное распространяться с помощью электронных писем
EXPLOIT	Эксплойт	Вредоносное ПО, использующее для развития атаки одну или несколько уязвимостей в целевом ПО. Применяется для запуска вредоносного кода без участия пользователя. Злоумышленники могут использовать его для повышения привилегий на устройстве
FLOODER	Флудильщик	Программа для отправки большого количества бесполезной информации по сетевым каналам. Может быть использована для рассылки спама, отвлечения внимания пользователя или обхода средств защиты
FRAUDTOOL	Инструмент для мошенничества	Программа, которая не выполняет заявленных функций. Может отвлекать пользователя или вводить его в заблуждение. Не является вредоносной, но может быть использована злоумышленниками
HACKTOOL	Пентест-инструменты	Инструмент, помогающий злоумышленнику развить атаку. Может использоваться для изменения параметров устройства, чтобы ослабить его защищенность, или для сокрытия действий атакующего. Применяется в тестировании на проникновение
HOAX	Программа-розыгрыш	Программа, предназначенная для демонстрации пользователю ложной, пугающей информации. Может злоупотреблять ресурсами ОС, причиняя неудобства и побуждая владельца устройства к необдуманным действиям (чаще всего злоумышленники используют такое ПО, чтобы обманом получить деньги пользователя)
IM_FLOODER	IM-флудильщик	Программа для отправки большого количества бесполезной информации через мессенджеры. Может быть использована для рассылки спама, отвлечения внимания пользователя или обхода средств защиты

Значение	Тип	Описание
IM_WORM	IM-червь	Вредоносное ПО, способное распространяться через мессенджеры
IRC_WORM	IRC-червь	Вредоносное ПО, способное распространяться через IRC (Internet Relay Chat)
MONITOR	Средство мониторинга	Программа для наблюдения за действиями пользователя. Применяется для трассировки активности ОС. Не является вредоносной, но может быть использована злоумышленниками
NET_WORM	Сетевой червь	Вредоносное ПО, способное распространяться без участия пользователя. Для этого используются уязвимости в ПО на новых узлах сети с последующим запуском вредоносного кода
NETTOOL	Сетевая утилита	Инструмент, выполняющий действия над сетевыми ресурсами в IT-инфраструктуре. Не является вредоносным ПО, чаще всего используется для сетевого администрирования, но злоумышленники могут применять его для развития атак
P2P_WORM	P2P-червь	Вредоносное ПО, способное распространяться через пиринговые сети
PHISHING	Фишинг	Рассылка с вредоносным содержанием, распространяемая через электронные письма или сообщения в мессенджерах. Злоумышленник обманным путем заставляет пользователя открыть присланный файл или перейти по ссылке. Если цель фишинга — кража средств, текст сообщения может содержать побуждение к выполнению денежных операций
PSWTOOL	Средство восстановления паролей	Программа для получения учетных данных пользователя и восстановления утраченной информации. Не является вредоносной, но может быть использована злоумышленниками
REMOTEADMIN	Средство удаленного доступа	Программа для удаленного управления устройством. Применяется для демонстрации действия пользователя или оказания услуг технической поддержки. Не является вредоносной, но может быть использована злоумышленниками
RISKTOOL	Потенциально нежелательное ПО	Инструмент для работы с локальными ресурсами устройства пользователя. Не является вредоносным ПО и чаще всего применяется для администрирования ОС, но, попав в руки злоумышленников, может нанести вред пользовательским данным

Значение	Тип	Описание
ROOTKIT	Руткит	Вредоносное ПО для сокрытия в системе объектов либо действий злоумышленника
SERVER_FTP	FTP-сервер	Удаленный компьютер, выполняющий функции FTP-сервера. Применяется для получения удаленного доступа к хранилищу данных на устройстве. Не является вредоносным ПО, но может быть использован злоумышленниками
SERVER_PROXY	Прокси-сервер	Удаленный компьютер, выполняющий функции прокси-сервера. Применяется для передачи данных через промежуточные узлы, когда пользователю нужно оставаться анонимным или отсутствует доступ к какой-либо сети. Не является вредоносным ПО, но может быть использован злоумышленниками
SERVER_TELNET	Telnet-сервер	Удаленный компьютер, выполняющий функции Telnet-сервера. Применяется для получения удаленного доступа к устройству пользователя. Не является вредоносным ПО, но может быть использован злоумышленниками
SERVER_WEB	Веб-сервер	Удаленный компьютер, выполняющий функции веб-сервера. Применяется для назначения устройству роли управляющего узла либо для получения доступа к информации. Не является вредоносным ПО, но может быть использован злоумышленниками
SMS_FLOODER	СМС-флудер	Программа для отправки большого количества бесполезной информации через SMS-сообщения. Может быть использована для рассылки спама, отвлечения внимания пользователя или обхода средств защиты
SPAM	Спам	Электронное письмо в составе массовой рассылки. Чаще всего содержит рекламное сообщение. Не несет ценной информации для пользователя
SPOOFER	Подмена	Программа для подмены идентификатора отправителя при отправке сетевых запросов. Применяется, чтобы скрыть адрес атакующего, помочь ему избежать обнаружения или легитимизировать выполняемые действия
TROJAN	Троян	Вредоносное ПО для совершения нелегитимных действий на устройстве пользователя (их невозможно классифицировать более точно). Не имеет возможностей для самораспространения

Значение	Тип	Описание
TROJAN_ARCBOMB	Архивная бомба	Вредоносное ПО, представляющее собой архив, при распаковке которого большая доля свободного пространства жесткого диска заполняется бесполезными или пустыми данными. Это может привести к замедлению работы устройства или к прекращению работы некоторых программ
TROJAN_BANKER	Банковский троян	Вредоносное ПО для кражи учетных данных пользователя, связанных с финансовыми системами, и передачи полученной информации злоумышленнику
TROJAN_CLICKER	Троян-кликер	Вредоносное ПО, симулирующее обращения к интернет-ресурсам. Используется для искусственной накрутки счетчиков посещений сайта с целью продвижения ресурса либо монетизации
TROJAN_DDOS	DDoS-бот	Вредоносное ПО для проведения распределенных атак типа «отказ в обслуживании». Компьютер пользователя автоматически становится звеном атаки. Злоумышленники могут настраивать ПО, чтобы изменить перечень целевых ресурсов
TROJAN_DOWNLOADER	Загрузчик ВПО	Вредоносное ПО для скачивания и запуска другого вредоносного ПО. Наиболее часто используемый класс вредоносного ПО для первичного заражения устройства
TROJAN_DROPPER	Установщик ВПО	Вредоносное ПО, извлекающее из своего тела и запускающее другое вредоносное ПО. Зачастую такая программа может установить вредоносное ПО нескольких классов
TROJAN_FAKEAV	Лжеанти-вирус	Вредоносное ПО, представляемое пользователю в качестве антивирусного продукта, но не являющееся таковым. Может требовать плату за использование, блокировать работу устройства, нарушать функционирование системы
TROJAN_GAMETHIEF	Средство кражи игровых учетных данных	Вредоносное ПО для кражи пользовательских данных в компьютерных и мобильных играх и передачи полученной информации злоумышленнику
TROJAN_IM	Средство кражи учетных	Вредоносное ПО для кражи пользовательских данных в мессенджерах и передачи полученной информации злоумышленнику

Значение	Тип	Описание
	данных мессен- джеров	
TROJAN_MAILFINDER	Сборщик адресов электрон- ной почты	Вредоносное ПО для сбора адресов электронной по- чты с устройства пользователя и передачи их зло- умышленнику
TROJAN_NOTIFIER	Троян-уве- домитель	Вредоносное ПО, уведомляющее злоумышленника об успешном заражении устройства. Не получает от зло- умышленника дополнительных компонентов или ко- манд
TROJAN_PROXY	Троян- прокси	Вредоносное ПО, предоставляющее злоумышленнику анонимный доступ в интернет через устройство поль- зователя либо туннелирующее сетевой трафик до недоступных извне узлов сети. Часто используется на стадии горизонтального перемещения либо для из- влечения важных данных при проведении атак
TROJAN_PSW	Средство кражи учетных данных	Вредоносное ПО для кражи учетных данных пользова- теля в системе или других программах и передачи по- лученной информации злоумышленнику
TROJAN_RANSOM	Троян-вы- могатель	Вредоносное ПО для вымогательской деятельности. Ценные файлы владельца устройства шифруются, а за их восстановление предлагается заплатить выкуп. В некоторых случаях те же файлы передаются злоумыш- леннику, чтобы усилить давление на пользователя и повысить шанс оплаты
TROJAN_SMS	СМС-тро- ян	Вредоносное ПО для отправки SMS-сообщений на номера, которые определяет злоумышленник. Может использоваться для подписки пользователя на плат- ные сервисы
TROJAN_SPY	Програм- ма-шпион	Вредоносное ПО для отслеживания действий пользо- вателя (перехват нажатых клавиш на клавиатуре, по- лучение изображения экрана, истории используемых программ, аудиозапись разговоров) и передачи полу- ченной информации злоумышленнику
UNKNOWN	—	Угроз не обнаружено
UNKNOWN_THREAT	—	Тип вредоносного ПО не указан

Значение	Тип	Описание
VIRTOOL	ПО для создания вирусов	Программа, которую злоумышленники используют для модификации вредоносного ПО, чтобы скрыть его от средств защиты. Применяются методы обфускации кода, шифрования данных или стеганографии. Может использоваться для заражения легитимного ПО
VIRUS	Вирус	Вредоносное ПО, способное распространяться среди локальных ресурсов пользователя
WEBTOOLBAR	Панель инструментов браузера	Панель инструментов, расширяющая возможности браузера. Иногда может получать доступ к значимым данным пользователя либо добавлять нежелательные возможности. Не является вредоносным ПО, но может быть использована злоумышленниками
WORM	Компьютерный червь	Вредоносное ПО, способное распространяться среди сетевых ресурсов пользователя

Глоссарий

Checkme

Служба для проверки объектов по электронной почте. Пользователь может отправить объект или переслать письмо на специальный электронный адрес и получить результат проверки в ответном письме.

анонимная проверка

Проверка объектов через веб-интерфейс без аутентификации в продукте.

белый список

Список хеш-сумм файлов, которые будут считаться безопасными при вынесении вердикта.

блокирующий режим

Режим проверки, при котором поступившие на проверку объекты блокируются продуктом до окончания проверки. В зависимости от вынесенного вердикта объект пропускается в информационную систему или удаляется (или помещается в карантин).

вердикт

Решение продукта о наличии или отсутствии угрозы в объекте, уровне опасности этой угрозы и типе представляющего угрозу вредоносного ПО.

динамический анализ

Совокупность методов проверки объекта, основанных на анализе его поведения. Имитируется взаимодействие пользователя с объектом и отслеживается появление связанных с этим угроз.

дочерний объект

Объект, выделенный продуктом из другого объекта. Например, при распаковке архива, извлечении ссылок из письма или скачивании контента по ссылке.

задание на проверку

Совокупность информации, связанной с поступившим на проверку объектом и действиями продукта по выявлению угроз в этом объекте.

индикатор компрометации

Объект или свойство объекта, которые указывают на связь рассматриваемой активности в сети организации с известными угрозами ИБ. Индикаторами компрометации могут быть, например, хеш-суммы файлов, доменные имена или IP-адреса.

источник для проверки

Интерфейс в информационной системе организации, с которого в продукт поступают объекты на проверку.

карточка задания

Страница в интерфейсе продукта с информацией о задании на проверку. На странице отображается информация об обнаруженных в задании угрозах и вынесенном по заданию вердикте.

карточка объекта

Страница в интерфейсе продукта с информацией об объекте задания. На странице отображается информация об используемых методах проверки, обнаруженных угрозах и вынесенном по объекту вердикте.

карточка поведенческого анализа

Страница в интерфейсе продукта с информацией о проверке файла задания методом поведенческого анализа.

наследуемый вердикт

Вердикт, вынесенный на основании результатов проверки дочерних объектов.

объект

Выделенный продуктом или полученный извне объем данных, для которого выполняется проверка на наличие угрозы. Например, файл, архив, письмо или ссылка.

опасный объект

Объект, который является вредоносным ПО и представляет угрозу для информационной системы или данных организации.

пассивный режим

Режим проверки, при котором поступившие на проверку объекты сразу пропускаются продуктом в информационную систему.

поведенческий анализ

Метод проверки объекта, основанный на анализе его поведения в изолированной виртуальной среде. Для выявления угроз в изолированной ОС имитируется взаимодействие пользователя с объектом и отслеживаются изменения, вносимые объектом в ОС и установленное ПО.

потенциально опасный объект

Объект, который при определенных обстоятельствах или действиях пользователя может представлять угрозу для информационной системы или данных организации.

прямой вердикт

Вердикт, вынесенный на основании результатов проверки самого объекта.

режим зеркалирования

Режим работы почтового сервера, при котором продукт не влияет на почтовый трафик сервера. На проверку в продукт отправляются копии писем.

режим ожидания

Режим проверки, при котором на проверку от источников в продукт поступают копии объектов, а их распространение контролирует пользователь или сторонняя система.

режим фильтрации

Режим работы почтового сервера, при котором продукт может фильтровать почтовый трафик сервера. В зависимости от выбранного режима проверки продукт либо сразу возвращает почтовому серверу отправленное на проверку письмо (пассивный режим), либо блокирует его до окончания проверки (блокирующий режим).

ретроспективный анализ

Метод проверки, заключающийся в регулярной повторной проверке объектов в хранилище. Использование обновленных средств проверки и антивирусных баз позволяет выявлять ранее неизвестные угрозы в уже проверенных объектах.

стандартный пароль

Пароль, который по умолчанию используется продуктом при распаковке отправленных на проверку зашифрованных архивов.

статический анализ

Совокупность методов проверки объектов, основанных на анализе их свойств и содержимого.

угроза

Возможность того, что информационной системе или данным организации будет нанесен вред. Угроза исходит от опасных и потенциально опасных объектов.

черный список

Список хеш-сумм файлов, которые будут считаться опасными при вынесении вердикта.



Positive Technologies — один из лидеров в области результативной кибербезопасности. Компания является ведущим разработчиком продуктов, решений и сервисов, позволяющих выявлять и предотвращать кибератаки до того, как они причинят неприемлемый ущерб бизнесу и целым отраслям экономики. Positive Technologies — первая и единственная компания из сферы кибербезопасности на Московской бирже (MOEX: POSI). Количество акционеров превышает 220 тысяч.



Email Security

версия 5.30

Руководство разработчика

© Positive Technologies, 2026.

Настоящий документ является собственностью Positive Technologies и защищен законодательством Российской Федерации и международными соглашениями об авторских правах и интеллектуальной собственности.

Копирование документа либо его фрагментов в любой форме, распространение, в том числе в переводе, а также их передача третьим лицам возможны только с письменного разрешения Positive Technologies.

Документ может быть изменен без предварительного уведомления.

Товарные знаки, использованные в тексте, приведены исключительно в информационных целях, исключительные права на них принадлежат соответствующим правообладателям.

Дата редакции документа: 06.02.2026

Содержание

1.	Об этом документе.....	5
1.1.	Условные обозначения.....	5
1.2.	Другие источники информации о PT Email Security.....	6
2.	Виды запросов к публичному API.....	7
2.1.	Работа с токенами доступа.....	7
2.2.	Проверка файлов и ссылок с передаваемыми параметрами.....	9
2.2.1.	Загрузка файла в PT Email Security для последующей проверки.....	10
2.2.2.	Запуск проверки файла.....	12
2.2.3.	Запуск проверки ссылки.....	20
2.2.4.	Получение общего результата проверки.....	30
2.2.5.	Получение подробных результатов проверки.....	32
2.3.	Проверка файлов и ссылок с параметрами источников.....	37
2.3.1.	Запуск проверки файла с выбранными параметрами.....	37
2.3.2.	Запуск проверки ссылки с выбранными параметрами.....	41
2.3.3.	Получение общего результата проверки.....	45
2.3.4.	Получение подробных результатов проверки.....	47
2.4.	Получение списка заданий.....	51
2.5.	Скачивание файла из хранилища.....	54
2.6.	Получение информации об образах виртуальных машин.....	55
2.7.	Получение состояния API.....	57
2.8.	Описание схем данных.....	58
2.8.1.	Схема ответа с результатами проверки.....	59
2.8.1.1.	Схема result.....	60
2.8.1.2.	Схема artifact.....	61
2.8.1.3.	Схема file_info.....	62
2.8.1.4.	Схема download_url_info.....	63
2.8.1.5.	Схема engine_result.....	63
2.8.1.6.	Схема log.....	65
2.8.1.7.	Схема network_object.....	65
2.8.1.8.	Схема error.....	66
2.8.2.	Схема ответа на неуспешный запрос.....	66
2.8.3.	Схема image.....	68
2.8.4.	Схема os.....	68
3.	Формат сообщений syslog.....	69
3.1.	Порядок отправки сообщений.....	69
3.2.	Типы данных полей.....	70
3.3.	Начало работы с источником.....	71
3.3.1.	Сообщение user_scan.start.....	72
3.3.2.	Сообщение check_me.start.....	74
3.3.3.	Сообщение email.start.....	78
3.3.4.	Сообщение mail_agent_mta.start.....	83
3.3.5.	Сообщение mail_bcc.start.....	87
3.3.6.	Сообщение mail_gateway.start.....	92

3.3.7.	Сообщение mail_gateway_mta.start	97
3.3.8.	Сообщение files_monitor.start	102
3.3.9.	Сообщение files_inbox.start	104
3.3.10.	Сообщение icap.start	106
3.3.11.	Сообщение dpi.start	113
3.3.12.	Сообщение retro.start	117
3.3.13.	Сообщение public_api.start	118
3.3.14.	Сообщение scan_api.start	120
3.3.15.	Сообщение pt_edr.start	122
3.4.	Добавление объекта, new_artifact	125
3.5.	Проверка объекта	133
3.5.1.	Сообщение scan_machine.new_object	134
3.5.2.	Сообщение scan_machine.file_result.av	139
3.5.3.	Сообщение scan_machine.file_result.pt_sandbox	145
3.5.4.	Сообщение scan_machine.file_result.melded	152
3.5.5.	Сообщение scan_machine.final_result	157
3.6.	Завершение работы с источником	160
3.6.1.	Сообщение user_scan.finish	162
3.6.2.	Сообщение check_me.finish	162
3.6.3.	Сообщение email.finish	163
3.6.4.	Сообщение mail_agent_mta.finish	164
3.6.5.	Сообщение mail_bcc.finish	166
3.6.6.	Сообщение mail_gateway.finish	166
3.6.7.	Сообщение mail_gateway_mta.finish	167
3.6.8.	Сообщение files_monitor.finish	169
3.6.9.	Сообщение files_inbox.finish	169
3.6.10.	Сообщение icap.finish	171
3.6.11.	Сообщение dpi.finish	172
3.6.12.	Сообщение retro.finish	173
3.6.13.	Сообщение public_api.finish	174
3.6.14.	Сообщение scan_api.finish	175
3.6.15.	Сообщение pt_edr.finish	175
3.7.	Обновление средства проверки, av.update	176
3.8.	События аудита, audit.event	177
3.9.	Типы источников	184
3.10.	Средства проверки	184
3.11.	Типы вредоносного ПО	185
4.	Создание пользовательского образа VM	192
4.1.	Установка и настройка VNC-сервера	193
4.2.	Создание образа VM из ISO-файла	193
4.3.	Создание образа VM из образа диска в формате QCOW2	196
4.4.	Копирование добавленного ранее образа VM	199
4.5.	Экспорт добавленного вручную пользовательского образа VM	202
4.6.	Ручная настройка ОС на образе VM	204
5.	О технической поддержке	208

1. Об этом документе

Руководство разработчика содержит информацию о доступных функциях сервиса публичного API, форматах сообщений syslog, отправляемых во внешние системы, и способах создания дополнительных образов виртуальных машин для поведенческого анализа файлов.

Руководство адресовано специалистам, выполняющим интеграцию PT Email Security со сторонними системами.

Комплект документации PT Email Security включает в себя следующие документы:

- Этот документ.
- Руководство по внедрению — содержит информацию для внедрения продукта в инфраструктуре организации: от описания типовых конфигураций до инструкций по установке и первоначальной настройке продукта.
- Руководство администратора — содержит справочную информацию и инструкции по настройке и администрированию продукта.
- Руководство специалиста по безопасности — содержит сценарии использования продукта для управления событиями информационной безопасности.
- Руководство пользователя — содержит инструкции по отправке файлов на проверку через интерфейс продукта или по электронной почте и просмотру результатов проверки.

В этом разделе

[Условные обозначения \(см. раздел 1.1\)](#)

[Другие источники информации о PT Email Security \(см. раздел 1.2\)](#)

1.1. Условные обозначения

В документе приняты условные обозначения.

Таблица 1. Условные обозначения

Пример	Описание
Внимание! При выключении модуля снижается уровень защищенности сети	Предупреждения. Содержат информацию о действиях или событиях, которые могут иметь нежелательные последствия
Примечание. Вы можете создать дополнительные отчеты	Примечания. Содержат советы, описания важных частных случаев, дополнительную или справочную информацию, которая может быть полезна при работе с продуктом
► Чтобы открыть файл:	Начало инструкции выделено специальным значком
Нажмите OK	Названия элементов интерфейса (например, кнопок, полей, пунктов меню) выделены полужирным шрифтом

Пример	Описание
Выполните команду <code>Stop-Service</code>	Текст командной строки, примеры кода, прочие данные, которые нужно ввести с клавиатуры, выделены специальным шрифтом. Также выделены специальным шрифтом имена файлов и пути к файлам и папкам
<code>Ctrl+Alt+Delete</code>	Комбинация клавиш. Чтобы использовать комбинацию, клавиши нужно нажимать одновременно
<Название программы>	Переменные заключены в угловые скобки

1.2. Другие источники информации о PT Email Security

Вы можете найти дополнительную информацию о PT Email Security [на портале технической поддержки](#).

Портал содержит статьи базы знаний, новости обновлений продуктов Positive Technologies, ответы на часто задаваемые вопросы пользователей. Для доступа к базе знаний и всем новостям нужно создать на портале учетную запись.

Если вы не нашли нужную информацию или решение проблемы самостоятельно, обратитесь [в службу технической поддержки \(см. раздел 5\)](#).

2. Виды запросов к публичному API

Взаимодействие между вашим приложением и публичным API продукта происходит по протоколу HTTPS. Метод запросов — POST (запрос `maintenance/checkHealth` допускается также отправлять методом GET).

Корневой URL API:

```
https://<Адрес PT Email Security>/api/v1
```

Любые параметры должны передаваться в теле запроса в формате JSON.

В ответ на запросы вашего приложения сервис возвращает сообщения в формате JSON.

В этом разделе

[Работа с токенами доступа \(см. раздел 2.1\)](#)

[Проверка файлов и ссылок с передаваемыми параметрами \(см. раздел 2.2\)](#)

[Проверка файлов и ссылок с параметрами источников \(см. раздел 2.3\)](#)

[Получение списка заданий \(см. раздел 2.4\)](#)

[Скачивание файла из хранилища \(см. раздел 2.5\)](#)

[Получение информации об образах виртуальных машин \(см. раздел 2.6\)](#)

[Получение состояния API \(см. раздел 2.7\)](#)

[Описание схем данных \(см. раздел 2.8\)](#)

2.1. Работа с токенами доступа

Токен доступа — это уникальная последовательность символов, которая используется для защиты PT Email Security от несанкционированного доступа через публичный API. Каждый запрос к публичному API должен содержать в поле заголовка `X-API-Key` токен доступа.

Примечание. Доступ к результатам проверки объекта и информации о задании вы можете получить только с тем же токеном доступа, с которым объект был отправлен на проверку.

Вы можете работать с токенами доступа при помощи консольных команд или через веб-интерфейс PT Email Security. В этом разделе описана работа с токенами доступа с помощью команд. Работа с токенами доступа через веб-интерфейс описана в Руководстве администратора.

Создание токена доступа

► Чтобы создать токен доступа,

выполните команду:

```
sudo ptmsctl api auth create <Название> -p <Разрешенное действие> -с "<Комментарий>"
```

Название должно содержать от 5 до 30 символов и быть уникальным среди названий всех токенов. Название может содержать только буквы латинского алфавита, цифры, дефис и при этом начинаться и заканчиваться только буквами.

В параметре `-p` или `--permissions` необходимо указать разрешенное действие: `SCAN_WITH_PREDEFINED_SETTINGS` — для проверки с параметрами источника, `SCAN_WITH_EXTENDED_SETTINGS` — для проверки с передаваемыми в запросе параметрами (по умолчанию) или `TASKS_VIEW_ALL` — для просмотра списка всех заданий и получения информации о любых заданиях.

Примечание. С помощью токена доступа с разрешенным действием `TASKS_VIEW_ALL` вы можете получать информацию о заданиях с помощью запросов `/analysis/checkTask`, `/analysis/listTasks`, `/analysis/report`.

В параметре `-c` или `--comment` можно добавить текстовый комментарий длиной не более 500 символов.

Например:

```
sudo ptmsctl api auth create example-token -p SCAN_WITH_PREDEFINED_SETTINGS
```

Примечание. Вы можете выбрать формат вывода результатов выполнения команды. Для этого после названия утилиты `ptmsctl` в параметре `-o` или `--output-format` необходимо указать один из форматов: `json`, `plain`, `table` (по умолчанию) или `yaml`.

Токен доступа создан. Появится информация о созданном токене доступа.

Таблица 2. Информация о токене доступа

Поле	Тип данных	Описание
<code>created</code>	String	UNIX-время создания токена доступа
<code>creator_login</code>	String	Логин пользователя, создавшего токен доступа
<code>comment</code>	String	Комментарий к токenu доступа
<code>name</code>	String	Название токена доступа
<code>permissions</code>	Enum	Разрешенное для токена доступа действие: — <code>SCAN_WITH_PREDEFINED_SETTINGS</code> — проверка объектов с параметрами источника; — <code>SCAN_WITH_EXTENDED_SETTINGS</code> — проверка объектов с передаваемыми в запросе параметрами; — <code>TASKS_VIEW_ALL</code> — просмотр списка всех заданий и получение информации о любых заданиях
<code>token</code>	String	Токен доступа.

Поле	Тип данных	Описание
		Внимание! Сохраните этот токен доступа для использования его в запросах к публичному API

Изменение комментария для токена доступа

- ▶ Чтобы изменить или добавить комментарий к уже созданному токenu доступа,

выполните команду:

```
sudo ptmsctl api auth update <Название> -c "<Комментарий>"
```

Например:

```
sudo ptmsctl api auth update example-token -c "Something about example token"
```

Комментарий изменен. Появится информация о токене доступа.

Просмотр списка действующих токенов доступа

- ▶ Чтобы просмотреть список действующих токенов доступа,

выполните команду:

```
sudo ptmsctl api auth list
```

Появится список с информацией о действующих токенах доступа.

Отзыв токена доступа

- ▶ Чтобы отозвать токен доступа,

выполните команду:

```
sudo ptmsctl api auth delete <Название>
```

Например:

```
sudo ptmsctl api auth delete example-token
```

Токен доступа отозван.

2.2. Проверка файлов и ссылок с передаваемыми параметрами

В этом разделе приводится описание запросов для отправки файлов и ссылок на проверку в PT Email Security с передаваемыми параметрами и получения результатов проверки при помощи публичного API.

В этом разделе

[Загрузка файла в PT Email Security для последующей проверки \(см. раздел 2.2.1\)](#)

[Запуск проверки файла \(см. раздел 2.2.2\)](#)

[Запуск проверки ссылки \(см. раздел 2.2.3\)](#)

[Получение общего результата проверки \(см. раздел 2.2.4\)](#)

[Получение подробных результатов проверки \(см. раздел 2.2.5\)](#)

2.2.1. Загрузка файла в PT Email Security для последующей проверки

Перед запуском проверки файла с помощью публичного API ваше приложение должно загрузить этот файл в PT Email Security.

Метод и URL запроса:

POST <Корневой URL API>/storage/uploadScanFile

Параметры запроса отсутствуют.

Файл нужно передавать в бинарном виде (MIME-тип — application/octet-stream) или через multipart/form-data. Каждый запрос может содержать только один файл.

Ответ на запрос

В ответ на успешный запрос сервис публичного API присылает сообщение с кодом 200. Тело ответного сообщения может содержать поля, описанные в таблице ниже.

Таблица 3. Поля в ответе на запрос на загрузку файла

Поле	Тип	Описание
file_uri	String	URI файла во внутреннем формате. URI можно использовать до удаления файла из хранилища (см. описание поля <code>t11</code> ниже)
t11	Integer	Время жизни файла в секундах после его загрузки. По истечении этого времени или после запуска проверки файла (см. раздел 2.2.2) PT Email Security удаляет файл из хранилища
errors	Array of JSON objects	Не заполняется

В ответ на неуспешный запрос сервис публичного API присылает ответ с кодом ошибки. Структура тела ответа соответствует [схеме ответа на неуспешный запрос \(см. раздел 2.8.2\)](#).

Возможные коды ошибок и их значения:

- 401 — в запросе нет токена доступа или он указан неверно;
- 405 — неправильно указан метод запроса;
- 413 — размер запроса превышает установленное ограничение.

Пример

Запрос:

```
POST /api/v1/storage/uploadScanFile
<Файл в бинарном формате>
```

Пример запроса в формате cURL:

- при передаче файла в бинарном формате:

```
curl -k https://<Адрес PT Email Security>/api/v1/storage/uploadScanFile -H "X-API-Key:<Сгенерированный токен доступа>" --data-binary @test.txt
```

- при передаче файла через multipart/form-data:

```
curl -k https://<Адрес PT Email Security>/api/v1/storage/uploadScanFile -H "X-API-Key:<Сгенерированный токен доступа>" -F "file=@test.txt"
```

Ответ на успешный запрос:

```
{
  "data": {
    "file_uri": "sfm-files:///2022-04-26-10/xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxxx/xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxxx",
    "ttl": 3600
  },
  "errors": []
}
```

Ответ на неуспешный запрос:

```
{
  "data": {},
  "errors": [
    {
      "message": "Authorization required",
      "type": "HTTPUnauthorized"
    }
  ]
}
```

2.2.2. Запуск проверки файла

Ваше приложение может запустить проверку файла, ранее [загруженного в продукт](#) (см. [раздел 2.2.1](#)), и в ответ получить результаты проверки и (или) идентификатор задания на проверку.

Метод и URL запроса:

POST <Корневой URL API>/analysis/createScanTask

Тело запроса может содержать параметры, описанные в таблице ниже.

Таблица 4. Параметры тела запроса на запуск проверки файла

Параметр	Обязательный	Тип	Описание
async_result	Нет	Boolean	Возвращать только идентификатор задания на проверку. Включение этого параметра может понадобиться для отправки асинхронных запросов на проверку файлов: ваше приложение может не дожидаться результатов проверки, а получать их отдельными запросами. Такие запросы позволяют получать результаты проверки как в общем виде (см. раздел 2.2.4), так и в подробном (см. раздел 2.2.5). Значение по умолчанию — false
file_name	Нет	String	Название проверяемого файла. Если название не указано, в веб-интерфейсе PT Email Security будет отображаться <Файл без названия>
file_uri	Да	String	Временный URI файла, полученный в одноименном параметре в ответе на запрос загрузки файла (см. раздел 2.2.1)
priority	Нет	Integer	Приоритет проверки от 1 до 4, где 4 — самый высокий приоритет. Значение по умолчанию — 3
short_result	Нет	Boolean	Возвращать только общий результат проверки. Значение false этого параметра игнорируется, если для параметра async_result используется значение true. Значение по умолчанию — true

Параметр	Обязательный	Тип	Описание
options			
analysis_depth	Нет	Integer	Глубина проверки. Максимальный уровень декомпозиции объектов с иерархической структурой (например, архивов, электронных писем и ссылок) или уровень декомпрессии сжатых файлов. При значении 0 проверка выполняется без декомпозиции и декомпрессии. Чем больше число, тем дольше может выполняться проверка. Допустимые значения: 0–100. По умолчанию — 0
cache_enabled	Нет	Boolean	Использовать ли результаты предыдущих проверок файлов методом поведенческого анализа (по умолчанию true)
mark_suspicious_files_options	Нет	JSON object	Дополнительные критерии определения потенциально опасных файлов
passwords_for_unpack	Нет	Array of strings	Список паролей для распаковки зашифрованных архивов
save_clean_files	Нет	Boolean	Сохранять ли в хранилище файлы без угроз (по умолчанию true)
url_extract_enabled	Нет	Boolean	Извлекать ли ссылки из объектов (по умолчанию false)
options → mark_suspicious_files_options			
encrypted_not_unpacked	Нет	Boolean	Определять как потенциально опасные зашифрованные и нераспакованные архивы
max_depth_exceeded	Нет	Boolean	Определять как потенциально опасные архивы с превышенной глубиной распаковки
office_encrypted	Нет	Boolean	Определять как потенциально опасные зашифрованные файлы офисных форматов
office_has_action	Нет	Boolean	Определять как потенциально опасные файлы офисных форматов с настроенными действиями (Actions). Примечание. Поддерживается только для файлов Microsoft Office версии 2007 или выше
office_has_active_x	Нет	Boolean	Определять как потенциально опасные файлы офисных форматов с элементами ActiveX.

Параметр	Обязательный	Тип	Описание
			Примечание. Поддерживается только для файлов Microsoft Office версии 2007 или выше
office_has_added_in	Нет	Boolean	Определять как потенциально опасные файлы офисных форматов надстройками Office
office_has_dde	Нет	Boolean	Определять как потенциально опасные файлы офисных форматов с функциями DDE. Примечание. Поддерживается только для файлов Microsoft Office версии 2007 или выше
office_has_embedded	Нет	Boolean	Определять как потенциально опасные файлы офисных форматов с внедренными объектами (OLE)
office_has_macros	Нет	Boolean	Определять как потенциально опасные файлы офисных форматов с макросами
office_has_remote_data	Нет	Boolean	Определять как потенциально опасные файлы офисных форматов с запросами к внешним данным. Примечание. Поддерживается только для файлов Microsoft Office версии 2007 или выше
office_has_remote_template	Нет	Boolean	Определять как потенциально опасные файлы офисных форматов, использующие шаблон. Примечание. Поддерживается только для файлов Microsoft Office версии 2007 или выше
pdf_encrypted	Нет	Boolean	Определять как потенциально опасные зашифрованные файлы PDF
pdf_has_action	Нет	Boolean	Определять как потенциально опасные файлы PDF с настроенными действиями (Actions)
pdf_has_embedded	Нет	Boolean	Определять как потенциально опасные файлы PDF с внедренными объектами (OLE)
pdf_has_javascript	Нет	Boolean	Определять как потенциально опасные файлы PDF со сценариями JavaScript
pdf_has_open_action	Нет	Boolean	Определять как потенциально опасные файлы PDF с настроенными действиями при открытии (OpenActions)
options → sandbox			
analysis_duration	Нет	Integer	Продолжительность наблюдения за файлом в ходе поведенческого анализа (в секундах).

Параметр	Обязательный	Тип	Описание
			Допустимые значения: 10–600. По умолчанию — 60
analysis_duration_bootkitmon	Нет	Integer	Продолжительность наблюдения за файлом в ходе поведенческого анализа после перезагрузки ОС (в секундах). Допустимые значения: 10–600. По умолчанию — 60
bootkitmon	Нет	Boolean	Выполнить поведенческий анализ файла с перезагрузкой ОС. Значение по умолчанию — false
custom_command	Нет	String	Команда для запуска файла при поведенческом анализе
enabled	Нет	Boolean	Выполнить поведенческий анализ. Значение по умолчанию — false
file_types	Нет	Array of strings	Типы и группы типов проверяемых файлов. По умолчанию проверяются все поддерживаемые типы файлов — ["adobe-acrobat/", "executable-files/", "presentations/", "spreadsheets/", "word-processor/"]
filter_by_properties	Нет	JSON object	Фильтрация файлов по группам типов с указанием дополнительных признаков. Архивы и файлы с указанными типами и дополнительными признаками будут отправляться на поведенческий анализ
filter_by_properties → office	Нет	Array of strings	Дополнительные признаки файлов офисных форматов для их отправки на поведенческий анализ. Возможные значения: — ENCRYPTED — зашифрованные; — HAS_ACTION — с настроенными действиями (Actions); — HAS_ACTIVE_X — с элементами ActiveX; — HAS_DDE — использующие функции динамического обмена данными; — HAS_EMBEDDED — с встроенными объектами; — HAS_MACROS — с макросами;

Параметр	Обязательный	Тип	Описание
			— HAS_REMOTE_DATA — с запросами к внешним данным; — HAS_REMOTE_TEMPLAT — использующие внешний шаблон
filter_by_properties → pdf	Нет	Array of strings	Дополнительные признаки файлов PDF для их отправки на поведенческий анализ. Возможные значения: — ENCRYPTED — зашифрованные; — HAS_ACTION — с настроенными действиями (Actions); — HAS_EMBEDDED — с встроенными объектами; — HAS_JAVASCRIPT — со сценариями JavaScript; — HAS_OPEN_ACTION — с настроенными действиями при открытии (OpenAction)
image_id	Да, если значение options → sandbox → enabled — true	String	Идентификатор образа виртуальной машины (см. раздел 2.6)
mitm_enabled	Нет	Boolean	Включить подмену сертификатов ПО сертификатами PT Email Security при расшифровке и анализе защищенного трафика. Значение по умолчанию — false
procdump_new_processes_on_finish	Нет	Boolean	Снимать дампы незавершенных процессов при завершении поведенческого анализа. Значение по умолчанию — false
save_video	Нет	Boolean	Включить запись видео поведенческого анализа. Значение по умолчанию — true

Ответ на запрос

В случае успешного выполнения запроса публичный API возвращает ответ с кодом 200 [по схеме ответа с результатами проверки](#) (см. [раздел 2.8.1](#)).

В ответ на неуспешный запрос сервис публичного API присылает ответ с кодом ошибки. Структура тела ответа соответствует [схеме ответа на неуспешный запрос](#) (см. раздел 2.8.2).

Возможные коды ошибок и их значения:

- 401 — в запросе нет токена доступа или он указан неверно;
- 404 — файл, URI которого указан в запросе, был удален из временного хранилища или этот URI указан с ошибкой;
- 405 — неправильно указан метод запроса.

Пример

Тело запроса на запуск синхронной проверки файла с выдачей подробных результатов проверки:

```
{
  "file_uri": "sfm-files:///2022-04-26-10/xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxx/
xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxx",
  "short_result": false
}
```

Тело запроса на запуск асинхронной проверки файла (с поведенческим анализом):

```
{
  "file_uri": "sfm-files:///2022-04-26-10/xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxx/
xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxx",
  "file_name": "installer.exe",
  "async_result": true,
  "options": {
    "analysis_depth": 3,
    "passwords_for_unpack": ["P@ssw0rd", "Administr@t0r", "checkpass"],
    "url_extract_enabled": false,
    "mark_suspicious_files_options": {
      "encrypted_not_unpacked": true,
      "max_depth_exceeded": true,
      "office_encrypted": true,
      "office_has_macros": true,
      "office_has_embedded": true,
      "office_has_active_x": true,
      "office_has_dde": true,
      "office_has_remote_data": true,
      "office_has_remote_template": true,
      "office_has_action": true,
      "pdf_encrypted": true,
      "pdf_has_embedded": true,
      "pdf_has_open_action": true,
      "pdf_has_action": true,
      "pdf_has_javascript": true
    }
  }
}
```

```

    },
    "sandbox": {
      "enabled": false,
      "image_id": "string",
      "file_types": [
        "adobe-acrobat/",
        "executable-files/",
        "presentations/",
        "spreadsheets/",
        "word-processor/"
      ],
      "custom_command": "string",
      "procdump_new_processes_on_finish": false,
      "analysis_duration": 60,
      "bootkitmon": false,
      "analysis_duration_bootkitmon": 60,
      "save_video": true,
      "mitm_enabled": false,
      "filter_by_properties": {
        "pdf": [
          "ENCRYPTED"
        ],
      }
    }
  }
}

```

Ответ на успешный асинхронный запрос (с включенным параметром `async_result`):

```

{
  "data": {
    "scan_id": "16d1f7aa-333a-4fe8-8637-786e2956233d"
  },
  "errors": []
}

```

Ответ на успешный синхронный запрос с подробными результатами проверки (с выключенными параметрами `async_result` и `short_result`):

```

{
  "data": {
    "artifacts": [
      {
        "artifacts": [],
        "engine_results": [
          {
            "database_time": 1618398601.0,
            "detections": [
              {

```



```

        "detect": "Win.Test.EICAR_HDB-1",
        "threat": "VIRUS"
    }
],
"engine_code_name": "clamav",
"engine_subsystem": "AV",
"engine_version": "0.102.2",
"result": {
    "errors": [],
    "scan_state": "FULL",
    "threat": "VIRUS",
    "verdict": "DANGEROUS"
}
},
{
    "database_time": 1617993482.0,
    "database_version": "1.0.0.552",
    "detections": [
        {
            "detect": "tool_win_ZZ_EICAR__Virus",
            "threat": "VIRUS"
        }
    ],
    "engine_code_name": "ptesc",
    "engine_subsystem": "STATIC",
    "engine_version": "0.0.0.1835+master",
    "result": {
        "errors": [],
        "scan_state": "FULL",
        "threat": "VIRUS",
        "verdict": "DANGEROUS"
    }
}
],
"file_info": {
    "file_path": "",
    "file_uri":
"sha256:215a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f",
    "md5": "44d88612fea8a7f36de82e1278abb02f",
    "mime_type": "text/plain; charset=us-ascii",
    "sha1": "3395856ce81f1b7382dee72602f798b642f14140",
    "sha256":
"275a021bbfb5489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f",
    "ssdeep": "12:I8UaTNFYsFb46LNVqIe4FIK2DrILX2VF9U/Vn4EAgQhrX/
3VVV3d0ZK000RX:/HjkITGIyuVJA5hrXfVVVtZd0d",
    "size": 69
},

```

```

    "result": {
      "errors": [],
      "scan_state": "FULL",
      "threat": "VIRUS",
      "verdict": "DANGEROUS"
    },
    "type": "FILE"
  }
],
"result": {
  "duration": 0.17754173884168268,
  "errors": [],
  "scan_state": "FULL",
  "threat": "VIRUS",
  "verdict": "DANGEROUS"
},
"scan_id": "16d1f7aa-333a-4fe8-8637-786e2956233d"
},
"errors": []
}

```

Ответ на неуспешный запрос:

```

{
  "data": {},
  "errors": [
    {
      "message": "File \\\sfm-files:///2022-04-26-10/xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx/xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx\" not found",
      "type": "HTTPNotFound"
    }
  ]
}

```

См. также

[Загрузка файла в PT Email Security для последующей проверки \(см. раздел 2.2.1\)](#)

[Получение информации об образах виртуальных машин \(см. раздел 2.6\)](#)

2.2.3. Запуск проверки ссылки

Ваше приложение может запустить проверку ссылки и в ответ получить результаты проверки и (или) идентификатор задания на проверку.

Метод и URL запроса:

POST <Корневой URL API>/analysis/createScanURLTask

Тело запроса может содержать параметры, описанные в таблице ниже.

Таблица 5. Параметры тела запроса на запуск проверки ссылки

Параметр	Обязательный	Тип	Описание
async_result	Нет	Boolean	Возвращать только идентификатор задания на проверку. Включение этого параметра может понадобиться для отправки асинхронных запросов на проверку ссылок: ваше приложение может не дожидаться результатов проверки, а получать их отдельными запросами. Такие запросы позволяют получать результаты проверки как в общем виде (см. раздел 2.2.4), так и в подробном (см. раздел 2.2.5). Значение по умолчанию — false
priority	Нет	Integer	Приоритет проверки от 1 до 4, где 4 — самый высокий приоритет. Значение по умолчанию — 3
short_result	Нет	Boolean	Возвращать только общий результат проверки. Значение false этого параметра игнорируется, если для параметра async_result используется значение true. Значение по умолчанию — true
url	Да	String	Проверяемая ссылка
options			
analysis_depth	Нет	Integer	Глубина проверки. Максимальный уровень декомпозиции объектов с иерархической структурой (например, архивов, электронных писем и ссылок) или уровень декомпрессии сжатых файлов. При значении 0 проверка выполняется без декомпозиции и декомпрессии. Чем больше число, тем дольше может выполняться проверка. Допустимые значения: 0–100. По умолчанию — 0
cache_enabled	Нет	Boolean	Использовать ли результаты предыдущих проверок файлов методом поведенческого анализа (по умолчанию true)

Параметр	Обязательный	Тип	Описание
mark_suspicious_files_options	Нет	JSON object	Дополнительные критерии определения потенциально опасных файлов
passwords_for_unpack	Нет	Array of strings	Список паролей для распаковки зашифрованных архивов
save_clean_files	Нет	Boolean	Сохранять ли в хранилище файлы без угроз (по умолчанию true)
url_extract_enabled	Нет	Boolean	Извлекать ли ссылки из объектов (по умолчанию false)
options → mark_suspicious_files_options			
encrypted_not_unpacked	Нет	Boolean	Определять как потенциально опасные зашифрованные и нераспакованные архивы
max_depth_exceeded	Нет	Boolean	Определять как потенциально опасные архивы с превышенной глубиной распаковки
office_encrypted	Нет	Boolean	Определять как потенциально опасные зашифрованные файлы офисных форматов
office_has_action	Нет	Boolean	Определять как потенциально опасные файлы офисных форматов с настроенными действиями (Actions). Примечание. Поддерживается только для файлов Microsoft Office версии 2007 или выше
office_has_active_x	Нет	Boolean	Определять как потенциально опасные файлы офисных форматов с элементами ActiveX. Примечание. Поддерживается только для файлов Microsoft Office версии 2007 или выше
office_has_add_in	Нет	Boolean	Определять как потенциально опасные файлы офисных форматов надстройками Office
office_has_dde	Нет	Boolean	Определять как потенциально опасные файлы офисных форматов с функциями DDE. Примечание. Поддерживается только для файлов Microsoft Office версии 2007 или выше

Параметр	Обязательный	Тип	Описание
office_has_embedded	Нет	Boolean	Определять как потенциально опасные файлы офисных форматов с внедренными объектами (OLE)
office_has_macros	Нет	Boolean	Определять как потенциально опасные файлы офисных форматов с макросами
office_has_remote_data	Нет	Boolean	Определять как потенциально опасные файлы офисных форматов с запросами к внешним данным. Примечание. Поддерживается только для файлов Microsoft Office версии 2007 или выше
office_has_remote_template	Нет	Boolean	Определять как потенциально опасные файлы офисных форматов, использующие шаблон. Примечание. Поддерживается только для файлов Microsoft Office версии 2007 или выше
pdf_encrypted	Нет	Boolean	Определять как потенциально опасные зашифрованные файлы PDF
pdf_has_action	Нет	Boolean	Определять как потенциально опасные файлы PDF с настроенными действиями (Actions)
pdf_has_embedded	Нет	Boolean	Определять как потенциально опасные файлы PDF с внедренными объектами (OLE)
pdf_has_javascript	Нет	Boolean	Определять как потенциально опасные файлы PDF со сценариями JavaScript
pdf_has_open_action	Нет	Boolean	Определять как потенциально опасные файлы PDF с настроенными действиями при открытии (OpenActions)
options → sandbox			
analysis_duration	Нет	Integer	Продолжительность наблюдения за файлом в ходе поведенческого анализа (в секундах). Допустимые значения: 10—600. По умолчанию — 60
analysis_duration_bootkitmon	Нет	Integer	Продолжительность наблюдения за файлом в ходе поведенческого анализа после перезагрузки ОС (в секундах).

Параметр	Обязательный	Тип	Описание
			Допустимые значения: 10—600. По умолчанию — 60
bootkitmon	Нет	Boolean	Выполнить поведенческий анализ файла с перезагрузкой ОС. Значение по умолчанию — false
custom_command	Нет	String	Команда для запуска файла при поведенческом анализе
enabled	Нет	Boolean	Выполнить поведенческий анализ. Значение по умолчанию — false
file_types	Нет	Array of strings	Типы и группы типов проверяемых файлов. По умолчанию проверяются все поддерживаемые типы файлов — ["adobe-acrobat/", "executable-files/", "presentations/", "spreadsheets/", "word-processor/"]
filter_by_properties	Нет	JSON object	Фильтрация файлов по группам типов с указанием дополнительных признаков. Архивы и файлы с указанными типами и дополнительными признаками будут отправляться на поведенческий анализ
filter_by_properties → office	Нет	Array of strings	Дополнительные признаки файлов офисных форматов для их отправки на поведенческий анализ. Возможные значения: — ENCRYPTED — зашифрованные; — HAS_ACTION — с настроенными действиями (Actions); — HAS_ACTIVE_X — с элементами ActiveX; — HAS_DDE — использующие функции динамического обмена данными; — HAS_EMBEDDED — с встроенными объектами; — HAS_MACROS — с макросами; — HAS_REMOTE_DATA — с запросами к внешним данным; — HAS_REMOTE_TEMPLAT — использующие внешний шаблон

Параметр	Обязательный	Тип	Описание
<code>filter_by_properties → pdf</code>	Нет	Array of strings	Дополнительные признаки файлов PDF для их отправки на поведенческий анализ. Возможные значения: — <code>ENCRYPTED</code> — зашифрованные; — <code>HAS_ACTION</code> — с настроенными действиями (Actions); — <code>HAS_EMBEDDED</code> — с встроенными объектами; — <code>HAS_JAVASCRIPT</code> — со сценариями JavaScript; — <code>HAS_OPEN_ACTION</code> — с настроенными действиями при открытии (OpenAction)
<code>image_id</code>	Да, если значение <code>options → sandbox → enabled — true</code>	String	Идентификатор образа виртуальной машины (см. раздел 2.6)
<code>mitm_enabled</code>	Нет	Boolean	Включить подмену сертификатов ПО сертификатами PT Email Security при расшифровке и анализе защищенного трафика. Значение по умолчанию — <code>false</code>
<code>procdump_new_processes_on_finish</code>	Нет	Boolean	Снимать дампы незавершенных процессов при завершении поведенческого анализа. Значение по умолчанию — <code>false</code>
<code>save_video</code>	Нет	Boolean	Включить запись видео поведенческого анализа. Значение по умолчанию — <code>true</code>

Ответ на запрос

В случае успешного выполнения запроса публичный API возвращает ответ с кодом 200 [по схеме ответа с результатами проверки](#) (см. раздел 2.8.1).

В ответ на неуспешный запрос сервис публичного API присылает ответ с кодом ошибки. Структура тела ответа соответствует [схеме ответа на неуспешный запрос](#) (см. раздел 2.8.2).

Возможные коды ошибок и их значения:

- 401 — в запросе нет токена доступа или он указан неверно;
- 403 — некорректный номер лицензии или для переданного в запросе токена доступа среди разрешенных действий не выбрана «Проверка с передаваемыми параметрами».

Пример

Тело запроса на запуск синхронной проверки ссылки с выдачей подробных результатов проверки:

```
{
  "url": http://example.ru,
  "short_result": false
}
```

Тело запроса на запуск асинхронной проверки ссылки (с поведенческим анализом):

```
{
  "url": http://example.ru,
  "async_result": true,
  "options": {
    "analysis_depth": 3,
    "passwords_for_unpack": ["P@ssw0rd", "Administr@t0r", "checkpass"],
    "url_extract_enabled": false,
    "mark_suspicious_files_options": {
      "encrypted_not_unpacked": true,
      "max_depth_exceeded": true,
      "office_encrypted": true,
      "office_has_macros": true,
      "office_has_embedded": true,
      "office_has_active_x": true,
      "office_has_dde": true,
      "office_has_remote_data": true,
      "office_has_remote_template": true,
      "office_has_action": true,
      "pdf_encrypted": true,
      "pdf_has_embedded": true,
      "pdf_has_open_action": true,
      "pdf_has_action": true,
      "pdf_has_javascript": true
    },
    "sandbox": {
      "enabled": false,
      "image_id": "string",
      "file_types": [
        "adobe-acrobat/",
        "executable-files/"
      ]
    }
  }
}
```



```

        "presentations/",
        "spreadsheets/",
        "word-processor/"
    ],
    "custom_command": "string",
    "procdump_new_processes_on_finish": false,
    "analysis_duration": 60,
    "bootkitmon": false,
    "analysis_duration_bootkitmon": 60,
    "save_video": true,
    "mitm_enabled": false,
    "filter_by_properties": {
        "pdf": [
            "ENCRYPTED"
        ],
    }
}
}
}
}

```

Ответ на успешный асинхронный запрос (с включенным параметром `async_result`):

```

{
  "data": {
    "scan_id": "16d1f7aa-333a-4fe8-8637-786e2956233d"
  },
  "errors": []
}

```

Ответ на успешный синхронный запрос с подробными результатами проверки (с выключенными параметрами `async_result` и `short_result`):

```

{
  "errors": [],
  "data": {
    "scan_id": "44c9cb78-74b5-11ee-8184-441ab5b46535",
    "result": {
      "scan_state": "FULL",
      "verdict": "DANGEROUS",
      "errors": [],
      "duration": 16.28870937973261,
      "threat": "VIRUS",
      "duration_full": 16.28870937973261
    },
    "artifacts": [
      {
        "artifacts": [
          {
            "artifacts": [],

```

```

"result": {
  "scan_state": "FULL",
  "errors": [],
  "verdict": "DANGEROUS",
  "threat": "VIRUS",
  "duration": 14.614,
  "duration_full": 14.712
},
"type": "FILE",
"file_info": {
  "file_uri":
"sha256:275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f",
  "file_path": "eicar.com",
  "mime_type": "text/plain; charset=us-ascii",
  "md5": "44d88612fea8a8f36de82e1278abb02f",
  "sha1": "3395856ce81f2b7382dee72602f798b642f14140",
  "sha256":
"275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f",
  "size": 68
},
"engine_results": [
  {
    "engine_code_name": "clamav",
    "engine_subsystem": "AV",
    "engine_version": "0.103.8",
    "database_time": 1698306473.0,
    "detections": [
      {
        "detect": "Eicar-Test-Signature",
        "threat": "VIRUS"
      }
    ],
    "result": {
      "scan_state": "FULL",
      "verdict": "DANGEROUS",
      "errors": [],
      "duration": 0.208,
      "duration_full": 0.293,
      "threat": "VIRUS"
    }
  },
  {
    "engine_code_name": "ptesc",
    "engine_subsystem": "STATIC",
    "engine_version": "5.6.0.61826",
    "database_time": 1698275624.0,
    "detections": [

```

```

        {
            "detect": "tool_multi_ZZ_EICAR__Virus",
            "threat": "VIRUS"
        }
    ],
    "database_version": "4.0.0.364",
    "result": {
        "scan_state": "FULL",
        "verdict": "DANGEROUS",
        "errors": [],
        "duration": 0.732,
        "duration_full": 0.8,
        "threat": "VIRUS"
    }
},
{
    "engine_code_name": "clamav",
    "engine_subsystem": "AV",
    "engine_version": "1.0.146.91321",
    "database_time": 1698392805.0,
    "detections": [
        {
            "detect": "Marker.Dos.EICAR-Test-File.dyb",
            "threat": "VIRUS"
        }
    ],
    "result": {
        "scan_state": "FULL",
        "verdict": "DANGEROUS",
        "errors": [],
        "duration": 14.493,
        "duration_full": 14.531,
        "threat": "VIRUS"
    }
}
],
"network_objects": []
}
],
"result": {
    "scan_state": "FULL",
    "errors": [],
    "verdict": "DANGEROUS",
    "threat": "VIRUS",
    "duration": 15.14,
    "duration_full": 15.151
}

```

```

    },
    "type": "URL",
    "file_info": {
        "file_uri": "sha256:",
        "file_path": "https://secure.eicar.org/eicar.com",
        "mime_type": "",
        "md5": "",
        "sha1": "",
        "sha256": "",
        "size": 0
    },
    "engine_results": [],
    "network_objects": []
}
]
}
}

```

Ответ на неуспешный запрос:

```

{
  "errors": [
    {
      "type": "ERROR_BAD_REQUEST",
      "message": "1 validation error for SchemaCreateScanURLTask\nurl\n field
required (type=value_error.missing)"
    }
  ],
  "data": {}
}

```

2.2.4. Получение общего результата проверки

Ваше приложение может получить общий результат проверки файла или ссылки при помощи отдельного запроса. Запрос можно использовать, когда проверка была запущена асинхронным методом (при помощи запроса `createScanTask` или `createScanURLTask` с включенным параметром `async_result`), который не подразумевает возвращения результатов проверки.

Метод и URL запроса:

POST <Корневой URL API>/analysis/checkTask

Тело запроса должно содержать параметр `scan_id` с идентификатором задания на проверку файла или ссылки.

Примечание. Ваше приложение может получить значение для параметра `scan_id` из ответа на [запрос проверки файла \(см. раздел 2.2.2\)](#) или [запрос проверки ссылки \(см. раздел 2.2.3\)](#). В этом случае идентификатор задания можно взять из поля `data` → `scan_id`.

Также тело запроса может содержать включенный параметр `allow_preflight` для получения в ответе предварительного результата проверки.

Ответ на запрос

В случае успешного выполнения запроса публичный API возвращает ответ с кодом 200 по [схеме ответа с результатами проверки \(см. раздел 2.8.1\)](#).

В ответ на неуспешный запрос сервис публичного API присылает ответ с кодом ошибки. Структура тела ответа соответствует [схеме ответа на неуспешный запрос \(см. раздел 2.8.2\)](#).

Возможные коды ошибок и их значения:

- 401 — в запросе нет токена доступа или он указан неверно;
- 404 — задание на проверку файла не найдено; возможно, оно было создано более трех часов назад и завершилось с ошибкой;
- 405 — неправильно указан метод запроса.

Пример

Тело запроса:

```
{ "scan_id": "16d1f7aa-333a-4fe8-8637-786e2956233d" }
```

Ответ, когда задание на проверку еще выполняется:

```
{
  "data": {
    "scan_id": "16d1f7aa-333a-4fe8-8637-786e2956233d"
  },
  "errors": []
}
```

Ответ, когда задание на проверку еще выполняется и есть предварительный результат (`allow_preflight=true`):

```
{
  "data": {
    "is_preflight": true,
    "result": {
      "duration": 0.177541738841683,
      "errors": [
      ],
      "scan_state": "FULL",
      "threat": "VIRUS",
      "verdict": "DANGEROUS"
    },
    "scan_id": "16d1f7aa-333a-4fe8-8637-786e2956233d"
  },
  "errors": [
  ]
}
```

```
]
}
```

Ответ, когда задание на проверку завершилось:

```
{
  "data": {
    "is_preflight": false,
    "result": {
      "duration": 0.17754173884168268,
      "errors": [],
      "scan_state": "FULL",
      "threat": "VIRUS",
      "verdict": "DANGEROUS"
    },
    "scan_id": "16d1f7aa-333a-4fe8-8637-786e2956233d"
  },
  "errors": []
}
```

Ответ на неуспешный запрос:

```
{
  "errors": [
    {
      "type": "ERROR_ITEM_NOT_FOUND",
      "message": "Item \"058f1426-b920-11eb-af49-e757f9105daf\" is not found here."
    }
  ],
  "data": {}
}
```

См. также

[Получение подробных результатов проверки \(см. раздел 2.2.5\)](#)

2.2.5. Получение подробных результатов проверки

Ваше приложение может получить детальные результаты проверки файла или ссылки при помощи отдельного запроса. Запрос можно использовать, когда проверка была запущена асинхронным методом (при помощи запроса `createScanTask` или `createScanURLTask` с включенным параметром `async_result`), который не подразумевает возвращения результатов проверки.

Метод и URL запроса:

```
POST <Корневой URL API>/analysis/report
```

Тело запроса должно содержать параметр `scan_id` с идентификатором задания на проверку файла или ссылки.

Примечание. Ваше приложение может получить значение для параметра `scan_id` из ответа [на запрос проверки файла \(см. раздел 2.2.2\)](#) или [на запрос проверки ссылки \(см. раздел 2.2.3\)](#). В этом случае идентификатор задания можно взять из поля `data` → `scan_id`.

Ответ на запрос

В случае успешного выполнения запроса публичный API возвращает ответ с кодом 200 [по схеме ответа с результатами проверки \(см. раздел 2.8.1\)](#).

В ответ на неуспешный запрос сервис публичного API присылает ответ с кодом ошибки. Структура тела ответа соответствует [схеме ответа на неуспешный запрос \(см. раздел 2.8.2\)](#).

Возможные коды ошибок и их значения:

- 401 — в запросе нет токена доступа или он указан неверно;
- 404 — задание на проверку файла не найдено; возможно, оно было создано более трех часов назад и завершилось с ошибкой;
- 405 — неправильно указан метод запроса.

Пример

Тело запроса:

```
{ "scan_id": "16d1f7aa-333a-4fe8-8637-786e2956233d" }
```

Ответ, когда задание на проверку еще выполняется:

```
{
  "data": {
    "scan_id": "16d1f7aa-333a-4fe8-8637-786e2956233d"
  },
  "errors": []
}
```

Ответ, когда задание на проверку завершилось:

```
{
  "data": {
    "artifacts": [
      {
        "artifacts": [],
        "engine_results": [
          {
            "database_time": 1618398601.0,
            "detections": [
              {
                "detect": "Win.Test.EICAR_HDB-1",
                "threat": "VIRUS"
              }
            ]
          }
        ]
      }
    ]
  }
}
```

```

    ],
    "engine_code_name": "clamav",
    "engine_subsystem": "AV",
    "engine_version": "0.102.2",
    "result": {
        "errors": [],
        "scan_state": "FULL",
        "threat": "VIRUS",
        "verdict": "DANGEROUS"
    }
},
{
    "database_time": 1617993482.0,
    "database_version": "1.0.0.552",
    "detections": [
        {
            "detect": "tool_win_ZZ_EICAR__Virus",
            "threat": "VIRUS"
        }
    ],
    "engine_code_name": "ptesc",
    "engine_subsystem": "STATIC",
    "engine_version": "0.0.0.1835+master",
    "result": {
        "errors": [],
        "scan_state": "FULL",
        "threat": "VIRUS",
        "verdict": "DANGEROUS"
    }
},
{
    "engine_code_name": "PT",
    "engine_subsystem": "SANDBOX",
    "details": {
        "sandbox": {
            "image": {
                "image_id": "win7-sp1-x64",
                "version": "1.0.0.144",
                "os": {
                    "architecture": "x64",
                    "locale": "ru-RU",
                    "name": "Microsoft Windows 7 Enterprise",
                    "service_pack": "sp1",
                    "version": "6.1.7601.18741"
                }
            }
        }
    }
},

```



```

    "artifacts": [
    ],
    "logs": [
      {
        "type": "EVENT_CORRELATED",
        "file_name": "events-correlated.log.gz",
        "file_uri":
"sha256:d88eb6f52506b8fdeffd37b98438949901055d47ad5298a99d68cbce77296d31"
      }
    ],
    "analysis_duration": 124.0,
    "network_objects": [
      {
        "type": "IP",
        "value": "93.184.216.34"
      },
      {
        "type": "DOMAIN",
        "value": "example.com"
      },
      {
        "type": "URL",
        "value": "http://example.com/"
      }
    ]
  }
}
},
{
  "file_info": {
    "file_path": "",
    "file_uri":
"sha256:215a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f",
    "md5": "44d88612fea8a7f36de82e1278abb02f",
    "mime_type": "text/plain; charset=us-ascii",
    "sha1": "3395856ce81f1b7382dee72602f798b642f14140",
    "sha256":
"275a021bbfb5489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f",
    "ssdeep": "12:I8UaTNFYsFb46LNVqIe4FIK2DrILX2VF9U/Vn4EAgQhrX/
3VVV3d0ZK00RX:/HjkITGIyuVJA5hrXfVVVtZd0d",
    "size": 69
  },
  "download_url_info": {
    "reason_phrase": "OK",
    "state": "FULL",
    "status_code": 200,
    "version": "5.x.x"
  }
}

```

```

    }
    "network_objects": [
      {
        "type": "URL",
        "value": "https://secure.eicar.org/eicar.com"
      }
    ],
    "result": {
      "errors": [],
      "scan_state": "FULL",
      "threat": "VIRUS",
      "verdict": "DANGEROUS"
    },
    "type": "FILE"
  }
],
"result": {
  "duration": 0.17754173884168268,
  "errors": [],
  "scan_state": "FULL",
  "threat": "VIRUS",
  "verdict": "DANGEROUS"
},
"scan_id": "16d1f7aa-333a-4fe8-8637-786e2956233d"
},
"errors": []
}

```

Ответ на неуспешный запрос:

```

{
  "errors": [
    {
      "type": "ERROR_ITEM_NOT_FOUND",
      "message": "Item \"058f1426-b920-11eb-af49-e757f9105daf\" is not found here."
    }
  ],
  "data": {}
}

```

См. также

[Получение общего результата проверки \(см. раздел 2.2.4\)](#)

2.3. Проверка файлов и ссылок с параметрами ИСТОЧНИКОВ

В этом разделе описываются запросы для проверки файлов и ссылок с использованием заранее настроенных в PT Email Security параметров проверки и получение результатов проверки при помощи публичного API.

Для использования запросов необходимо в веб-интерфейсе PT Email Security создать токен доступа с соответствующим разрешенным действием и добавить источник для проверки с типом «API с выбранными параметрами проверки». Создание токена доступа и источника для проверки описано в Руководстве администратора.

Кроме того, PT Email Security может получать для проверки через публичный API файлы конечных устройств от MaxPatrol EDR.

Для использования запросов необходимо в веб-интерфейсе PT Email Security создать токен доступа с соответствующим разрешенным действием и добавить источник для проверки с типом «MaxPatrol EDR». В заголовке запроса необходимо передавать `X-Source-Product="EDR"`. Создание токена доступа и источника для проверки описано в Руководстве администратора.

В этом разделе

[Запуск проверки файла с выбранными параметрами \(см. раздел 2.3.1\)](#)

[Запуск проверки ссылки с выбранными параметрами \(см. раздел 2.3.2\)](#)

[Получение общего результата проверки \(см. раздел 2.3.3\)](#)

[Получение подробных результатов проверки \(см. раздел 2.3.4\)](#)

2.3.1. Запуск проверки файла с выбранными параметрами

Ваше приложение может запустить проверку файла с заранее выбранными параметрами и в ответ получить результаты проверки и (или) идентификатор задания на проверку.

Метод и URL запроса:

POST <Корневой URL API>/scan/checkFile

Таблица 6. Параметры запроса на запуск проверки файла

Параметр	Обязательный	Тип	Описание
async_result	Нет	Boolean	Возвращать только идентификатор задания на проверку. Включение этого параметра может понадобиться для отправки асинхронных запросов на проверку файлов: ваше приложение может не дожидаться результатов про-

Параметр	Обязательный	Тип	Описание
			верки, а получать их отдельными запросами. Такие запросы позволяют получать результаты проверки как в общем виде (см. раздел 2.2.4) , так и в подробном (см. раздел 2.2.5) . Значение по умолчанию — <code>false</code>
<code>file_name</code>	Нет	String	Название проверяемого файла. Если название не указано, в веб-интерфейсе PT Email Security будет отображаться <Файл без названия>
<code>passwords_for_unpack</code>	Нет	Array of strings	Список паролей для распаковки зашифрованных архивов
<code>priority</code>	Нет	Integer	Приоритет проверки от 1 до 4, где 4 — самый высокий приоритет. Значение по умолчанию — 3
<code>short_result</code>	Нет	Boolean	Возвращать только общий результат проверки. Значение <code>false</code> этого параметра игнорируется, если для параметра <code>async_result</code> используется значение <code>true</code> . Значение по умолчанию — <code>true</code>

Файл нужно передавать в бинарном виде (MIME-тип — `application/octet-stream`) или через `multipart/form-data`. Каждый запрос может содержать только один файл.

Ответ на запрос

В случае успешного выполнения запроса публичный API возвращает ответ с кодом 200 [по схеме ответа с результатами проверки \(см. раздел 2.8.1\)](#).

В ответ на неуспешный запрос сервис публичного API присылает ответ с кодом ошибки. Структура тела ответа соответствует [схеме ответа на неуспешный запрос \(см. раздел 2.8.2\)](#).

Возможные коды ошибок и их значения:

- 401 — в запросе нет токена доступа, он указан неверно или не привязан к источнику с типом «API с выбранными параметрами проверки»;
- 403 — для переданного в запросе токена доступа среди разрешенных действий не выбрана «Проверка с параметрами источника»;
- 413 — размер запроса превышает установленное ограничение.

Пример

Тело запроса на запуск синхронной проверки файла с выдачей подробных результатов проверки:

```
POST /api/v1/scan/checkFile?
file_name=some_file.exe&short_result=true&async_result=false&priority=1
<Файл в бинарном формате>
```

Пример запроса в формате cURL:

— при передаче файла в бинарном формате:

```
curl -k https://<Адрес PT Email Security>/api/v1/scan/checkFile?file_name=some-
name.txt -H "X-API-Key:<Сгенерированный токен доступа>" --data-binary @test.txt
```

— при передаче файла в multipart/form-data:

```
curl -k https://<Адрес PT Email Security>/api/v1/scan/checkFile?file_name=some-
name.txt -H "X-API-Key:<Сгенерированный токен доступа>" -F "file=@test.txt"
```

Ответ на успешный асинхронный запрос (с включенным параметром `async_result`):

```
{
  "data": {
    "scan_id": "16d1f7aa-333a-4fe8-8637-786e2956233d"
  },
  "errors": []
}
```

Ответ на успешный синхронный запрос с подробными результатами проверки (с выключенными параметрами `async_result` и `short_result`):

```
{
  "data": {
    "artifacts": [
      {
        "artifacts": [],
        "engine_results": [
          {
            "database_time": 1618398601.0,
            "detections": [
              {
                "detect": "Win.Test.EICAR_HDB-1",
                "threat": "VIRUS"
              }
            ],
            "engine_code_name": "clamav",
            "engine_subsystem": "AV",
            "engine_version": "0.102.2",
            "result": {
              "errors": [],
              "scan_state": "FULL",

```

```

        "threat": "VIRUS",
        "verdict": "DANGEROUS"
    }
},
{
    "database_time": 1617993482.0,
    "database_version": "1.0.0.552",
    "detections": [
        {
            "detect": "tool_win_ZZ_EICAR__Virus",
            "threat": "VIRUS"
        }
    ],
    "engine_code_name": "ptesc",
    "engine_subsystem": "STATIC",
    "engine_version": "0.0.0.1835+master",
    "result": {
        "errors": [],
        "scan_state": "FULL",
        "threat": "VIRUS",
        "verdict": "DANGEROUS"
    }
}
],
"file_info": {
    "file_path": "",
    "file_uri":
"sha256:215a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f",
    "md5": "44d88612fea8a7f36de82e1278abb02f",
    "mime_type": "text/plain; charset=us-ascii",
    "sha1": "3395856ce81f1b7382dee72602f798b642f14140",
    "sha256":
"275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f",
    "ssdeep": "12:I8UaTNFYsFb46LNVqIe4FIK2DrILX2VF9U/Vn4EAgQhrX/
3VVV3d0ZK000RX:/HjkITGIyuVJA5hrXfVVVtZd0d",
    "size": 69
},
"result": {
    "errors": [],
    "scan_state": "FULL",
    "threat": "VIRUS",
    "verdict": "DANGEROUS"
},
"type": "FILE"
}
],
"result": {

```

```

    "duration": 0.17754173884168268,
    "errors": [],
    "scan_state": "FULL",
    "threat": "VIRUS",
    "verdict": "DANGEROUS"
  },
  "scan_id": "16d1f7aa-333a-4fe8-8637-786e2956233d"
},
"errors": []
}

```

Ответ на неуспешный запрос:

```

{
  "errors": [
    {
      "type": "HTTPUnauthorized",
      "message": "PublicAPI endpoint \"api-entrypoint-name\" disabled"
    }
  ],
  "data": {}
}

```

2.3.2. Запуск проверки ссылки с выбранными параметрами

Ваше приложение может запустить проверку ссылки и в ответ получить результаты проверки и (или) идентификатор задания на проверку.

Метод и URL запроса:

POST <Корневой URL API>/scan/checkURL

Таблица 7. Параметры запроса на запуск проверки ссылки

Параметр	Обязательный	Тип	Описание
passwords_for_unpack	Нет	Array of strings	Список паролей для распаковки зашифрованного архива по ссылке

Тело запроса может содержать параметры, описанные в таблице ниже.

Таблица 8. Параметры тела запроса на запуск проверки ссылки

Параметр	Обязательный	Тип	Описание
url	Да	String	Проверяемая ссылка

Параметр	Обязательный	Тип	Описание
<code>async_result</code>	Нет	Boolean	Возвращать только идентификатор задания на проверку. Включение этого параметра может понадобиться для отправки асинхронных запросов на проверку ссылок: ваше приложение может не дожидаться результатов проверки, а получать их отдельными запросами. Такие запросы позволяют получать результаты проверки как в общем виде (см. раздел 2.2.4) , так и в подробном (см. раздел 2.2.5) . Значение по умолчанию — <code>false</code>
<code>priority</code>	Нет	Integer	Приоритет проверки от 1 до 4, где 4 — самый высокий приоритет. Значение по умолчанию — 3
<code>short_result</code>	Нет	Boolean	Возвращать только общий результат проверки. Значение <code>false</code> этого параметра игнорируется, если для параметра <code>async_result</code> используется значение <code>true</code> . Значение по умолчанию — <code>true</code>

Ответ на запрос

В случае успешного выполнения запроса публичный API возвращает ответ с кодом 200 [по схеме ответа с результатами проверки \(см. раздел 2.8.1\)](#).

В ответ на неуспешный запрос сервис публичного API присылает ответ с кодом ошибки. Структура тела ответа соответствует [схеме ответа на неуспешный запрос \(см. раздел 2.8.2\)](#).

Возможные коды ошибок и их значения:

- 401 — в запросе нет токена доступа, он указан неверно или не привязан к источнику с типом «API с выбранными параметрами проверки»;
- 403 — для переданного в запросе токена доступа среди разрешенных действий не выбрана «Проверка с параметрами источника»;
- 413 — размер запроса превышает установленное ограничение.

Пример

Тело запроса на запуск синхронной проверки ссылки с выдачей подробных результатов проверки:

```
{
  "url": http://example.ru,
  "short_result": false
}
```

Ответ на успешный асинхронный запрос (с включенным параметром `async_result`):

```
{
  "data": {
    "scan_id": "16d1f7aa-333a-4fe8-8637-786e2956233d"
  },
  "errors": []
}
```

Ответ на успешный синхронный запрос с подробными результатами проверки (с выключенными параметрами `async_result` и `short_result`):

```
{
  "data": {
    "artifacts": [
      {
        "artifacts": [],
        "engine_results": [
          {
            "database_time": 1618398601.0,
            "detections": [
              {
                "detect": "Win.Test.EICAR_HDB-1",
                "threat": "VIRUS"
              }
            ],
            "engine_code_name": "clamav",
            "engine_subsystem": "AV",
            "engine_version": "0.102.2",
            "result": {
              "errors": [],
              "scan_state": "FULL",
              "threat": "VIRUS",
              "verdict": "DANGEROUS"
            }
          }
        ],
        "database_time": 1617993482.0,
        "database_version": "1.0.0.552",

```

```

    "detections": [
      {
        "detect": "tool_win_ZZ_EICAR__Virus",
        "threat": "VIRUS"
      }
    ],
    "engine_code_name": "ptesc",
    "engine_subsystem": "STATIC",
    "engine_version": "0.0.0.1835+master",
    "result": {
      "errors": [],
      "scan_state": "FULL",
      "threat": "VIRUS",
      "verdict": "DANGEROUS"
    }
  },
  "file_info": {
    "file_path": "",
    "file_uri":
"sha256:215a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f",
    "md5": "44d88612fea8a7f36de82e1278abb02f",
    "mime_type": "text/plain; charset=us-ascii",
    "sha1": "3395856ce81f1b7382dee72602f798b642f14140",
    "sha256":
"275a021bbfb5489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f",
    "ssdeep": "12:I8UaTNFYsFb46LNVqIe4FIK2DrILX2VF9U/Vn4EAgQhrX/
3VVV3d0ZK000RX:/HjkITGIyuVJA5hrXfVVVtZd0d",
    "size": 69
  },
  "result": {
    "errors": [],
    "scan_state": "FULL",
    "threat": "VIRUS",
    "verdict": "DANGEROUS"
  },
  "type": "FILE"
},
"result": {
  "duration": 0.17754173884168268,
  "errors": [],
  "scan_state": "FULL",
  "threat": "VIRUS",
  "verdict": "DANGEROUS"
},
"scan_id": "16d1f7aa-333a-4fe8-8637-786e2956233d"

```

```
    },
    "errors": []
  }
}
```

Ответ на неуспешный запрос:

```
{
  "errors": [
    {
      "type": "HTTPUnauthorized",
      "message": "PublicAPI endpoint \"api-entrypoint-name\" disabled"
    }
  ],
  "data": {}
}
```

2.3.3. Получение общего результата проверки

Ваше приложение может получить общий результат проверки файла или ссылки при помощи отдельного запроса. Запрос можно использовать, когда проверка была запущена асинхронным методом (при помощи запроса `scan/checkFile` или `scan/checkURL` с включенным параметром `async_result`), который не подразумевает возвращения результатов проверки.

Метод и URL запроса:

```
POST <Корневой URL API>/scan/getStatus
```

Тело запроса должно содержать параметр `scan_id` с идентификатором задания на проверку файла или ссылки.

Примечание. Ваше приложение может получить значение для параметра `scan_id` из ответа на [запрос проверки файла \(см. раздел 2.3.1\)](#) или на [запрос проверки ссылки \(см. раздел 2.3.2\)](#). В этом случае идентификатор задания можно взять из поля `data` → `scan_id`.

Также тело запроса может содержать включенный параметр `allow_preflight` для получения в ответе предварительного результата проверки.

Ответ на запрос

В случае успешного выполнения запроса публичный API возвращает ответ с кодом 200 по [схеме ответа с результатами проверки \(см. раздел 2.8.1\)](#).

В ответ на неуспешный запрос сервис публичного API присылает ответ с кодом ошибки. Структура тела ответа соответствует [схеме ответа на неуспешный запрос \(см. раздел 2.8.2\)](#).

Возможные коды ошибок и их значения:

- 401 — в запросе нет токена доступа или он указан неверно;
- 404 — задание на проверку файла не найдено; возможно, оно было создано более трех часов назад и завершилось с ошибкой;
- 405 — неправильно указан метод запроса.

Пример

Тело запроса:

```
{ "scan_id": "16d1f7aa-333a-4fe8-8637-786e2956233d" }
```

Ответ, когда задание на проверку еще выполняется и есть предварительный результат (allow_preflight=true):

```
{
  "data": {
    "is_preflight": true,
    "result": {
      "duration": 0.177541738841683,
      "errors": [
      ],
      "scan_state": "FULL",
      "threat": "VIRUS",
      "verdict": "DANGEROUS"
    },
    "scan_id": "16d1f7aa-333a-4fe8-8637-786e2956233d"
  },
  "errors": [
  ]
}
```

Ответ, когда задание на проверку завершилось (с включенным параметром allow_preflight):

```
{
  "data": {
    "is_preflight": false,
    "result": {
      "duration": 0.17754173884168268,
      "errors": [
      ],
      "scan_state": "FULL",
      "threat": "VIRUS",
      "verdict": "DANGEROUS"
    },
    "scan_id": "16d1f7aa-333a-4fe8-8637-786e2956233d"
  },
  "errors": [
  ]
}
```

Ответ на неуспешный запрос:

```
{
  "errors": [
    {
      "type": "ERROR_ITEM_NOT_FOUND",
      "message": "Item \"058f1426-b920-11eb-af49-e757f9105daf\" is not found here."
    }
  ],
  "data": {}
}
```

2.3.4. Получение подробных результатов проверки

Ваше приложение может получить детальные результаты проверки файла или ссылки при помощи отдельного запроса. Запрос можно использовать, когда проверка была запущена асинхронным методом (при помощи запроса `scan/checkFile` или `scan/checkURL` с включенным параметром `async_result`), который не подразумевает возвращения результатов проверки.

Метод и URL запроса:

POST <Корневой URL API>/scan/getFullReport

Тело запроса должно содержать параметр `scan_id` с идентификатором задания на проверку файла или ссылки.

Примечание. Ваше приложение может получить значение для параметра `scan_id` из ответа на [запрос проверки файла \(см. раздел 2.3.1\)](#) или на [запрос проверки ссылки \(см. раздел 2.3.2\)](#). В этом случае идентификатор задания можно взять из поля `data` → `scan_id`.

Ответ на запрос

В случае успешного выполнения запроса публичный API возвращает ответ с кодом 200 по [схеме ответа с результатами проверки \(см. раздел 2.8.1\)](#).

В ответ на неуспешный запрос сервис публичного API присылает ответ с кодом ошибки. Структура тела ответа соответствует [схеме ответа на неуспешный запрос \(см. раздел 2.8.2\)](#).

Возможные коды ошибок и их значения:

- 401 — в запросе нет токена доступа или он указан неверно;
- 404 — задание на проверку файла не найдено; возможно, оно было создано более трех часов назад и завершилось с ошибкой;
- 405 — неправильно указан метод запроса.

Пример

Тело запроса:

```
{ "scan_id": "16d1f7aa-333a-4fe8-8637-786e2956233d" }
```

Ответ, когда задание на проверку еще выполняется:

```
{
  "data": {
    "scan_id": "16d1f7aa-333a-4fe8-8637-786e2956233d"
  },
  "errors": []
}
```

Ответ, когда задание на проверку завершилось:

```
{
  "data": {
    "artifacts": [
      {
        "artifacts": [],
        "engine_results": [
          {
            "database_time": 1618398601.0,
            "detections": [
              {
                "detect": "Win.Test.EICAR_HDB-1",
                "threat": "VIRUS"
              }
            ],
            "engine_code_name": "clamav",
            "engine_subsystem": "AV",
            "engine_version": "0.102.2",
            "result": {
              "errors": [],
              "scan_state": "FULL",
              "threat": "VIRUS",
              "verdict": "DANGEROUS"
            }
          }
        ],
        {
          "database_time": 1617993482.0,
          "database_version": "1.0.0.552",
          "detections": [
            {
              "detect": "tool_win_ZZ_EICAR__Virus",
              "threat": "VIRUS"
            }
          ]
        }
      ]
    }
  }
}
```

```

    ],
    "engine_code_name": "ptesc",
    "engine_subsystem": "STATIC",
    "engine_version": "0.0.0.1835+master",
    "result": {
      "errors": [],
      "scan_state": "FULL",
      "threat": "VIRUS",
      "verdict": "DANGEROUS"
    }
  },
  {
    "engine_code_name": "PT",
    "engine_subsystem": "SANDBOX",
    "details": {
      "sandbox": {
        "image": {
          "image_id": "win7-sp1-x64",
          "version": "1.0.0.144",
          "os": {
            "architecture": "x64",
            "locale": "ru-RU",
            "name": "Microsoft Windows 7 Enterprise",
            "service_pack": "sp1",
            "version": "6.1.7601.18741"
          }
        }
      },
      "artifacts": [
      ],
      "logs": [
        {
          "type": "EVENT_CORRELATED",
          "file_name": "events-correlated.log.gz",
          "file_uri":
"sha256:d88eb6f52506b8fdeffd37b98438949901055d47ad5298a99d68cbce77296d31"
        }
      ],
      "analysis_duration": 124.0,
      "network_objects": [
        {
          "type": "IP",
          "value": "93.184.216.34"
        },
        {
          "type": "DOMAIN",
          "value": "example.com"
        }
      ]
    }
  }
]

```

```

        },
        {
            "type": "URL",
            "value": "http://example.com/"
        }
    ]
}
}
}
},
],
"file_info": {
    "file_path": "",
    "file_uri":
"sha256:215a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f",
    "md5": "44d88612fea8a7f36de82e1278abb02f",
    "mime_type": "text/plain; charset=us-ascii",
    "sha1": "3395856ce81f1b7382dee72602f798b642f14140",
    "sha256":
"275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f",
    "ssdeep": "12:I8UaTNFYsFb46LNVqIe4FIK2DrILX2VF9U/Vn4EAgQhrX/
3VVV3d0ZK000RX:/HjkITGIyuVJA5hrXfVVVtZd0d",
    "size": 69
},
"download_url_info": {
    "reason_phrase": "OK",
    "state": "FULL",
    "status_code": 200,
    "version": "5.x.x"
}
"network_objects": [
    {
        "type": "URL",
        "value": "https://secure.eicar.org/eicar.com"
    }
],
"result": {
    "errors": [],
    "scan_state": "FULL",
    "threat": "VIRUS",
    "verdict": "DANGEROUS"
},
"type": "FILE"
}
],
"result": {
    "duration": 0.17754173884168268,
    "errors": [],

```



```

        "scan_state": "FULL",
        "threat": "VIRUS",
        "verdict": "DANGEROUS"
    },
    "scan_id": "16d1f7aa-333a-4fe8-8637-786e2956233d"
},
"errors": []
}

```

Ответ на неуспешный запрос:

```

{
  "errors": [
    {
      "type": "ERROR_ITEM_NOT_FOUND",
      "message": "Item \"058f1426-b920-11eb-af49-e757f9105daf\" is not found here."
    }
  ],
  "data": {}
}

```

2.4. Получение списка заданий

Запрос для просмотра списка заданий и получения информации о заданиях.

Метод и URL запроса:

POST <Корневой URL API>/analysis/listTasks

Тело запроса:

```

{
  "limit": <Integer>,
  "next_cursor": "<String>",
  "query": "<String>",
  "utc_offset_seconds": <Integer>,
}

```

Тело запроса может содержать параметры, описанные в таблице.

Таблица 9. Параметры в теле запроса на получение списка заданий

Параметр	Обязатель- ный	Тип	Описание
limit	—	Integer	Количество заданий в ответе, не более 200 (по умолчанию 20)
next_cursor	—	String	Порядковый номер задания. Содержится в ответе на предыдущий запрос в поле next_cursor

Параметр	Обязательный	Тип	Описание
query	—	String	QL-запрос для фильтрации заданий
utc_offset_secons	—	Integer	Смещение времени QL-запроса относительно UTC в часах (по умолчанию 0)

Ответ на запрос

В ответ на успешный запрос сервис публичного API присылает ответ с кодом 200.

Тело ответа:

```
{
  "next_cursor": "<String>",
  "tasks": [
    <JSON object 1>,
    <JSON object 2>,
    ...
  ]
}
```

Тело ответа содержит поля, описанные в таблице.

Таблица 10. Поля в теле ответа на запрос на получение списка заданий

Поле	Тип	Описание
next_cursor	String	Порядковый номер задания для следующего запроса. Если значение не указано, отправлены данные обо всех заданиях
tasks	Array of JSON objects	Информация о заданиях

tasks → <JSON object>

<pre>{ "duration": <Float>, "duration_full": <Float>, "entry_point_id": "<String>", "entry_point_type": "<String>", "id": "<String>", "name": "<String>", "scan_state": "<Enum>", "start_time": <Float>, "threat": "<Enum>", "verdict": "<Enum>" }</pre>		
duration	Float	Продолжительность проверки в секундах

Поле	Тип	Описание
duration_full	Float	Общая продолжительность проверки от запроса до записи результатов в секундах
entry_point_id	String	Название источника
entry_point_type	String	Тип источника
id	String	Идентификатор задания
name	String	Название задания
scan_state	Enum	Статус проверки задания: — FULL — проверка выполнена полностью; — PARTIAL — выполнена частично; — UNSCANNED — не выполнена
start_time	Float	Время создания задания
threat	String	Тип вредоносного ПО (см. раздел 3.11)
verdict	Enum	Уровень опасности объекта задания: — CLEAN — без обнаруженных угроз; — DANGEROUS — опасный объект; — UNWANTED — потенциально опасный объект

В ответ на неуспешный запрос сервис публичного API присылает ответ с кодом ошибки. Структура тела ответа соответствует [схеме ответа на неуспешный запрос \(см. раздел 2.8.2\)](#).

Возможные коды ошибок и их значения:

- 401 (Unauthorized) — ошибка аутентификации, требуется действующий токен доступа.
- 403 (Forbidden) — недействительная лицензия или переданному в запросе токenu доступа не разрешено действие, необходимое для выполнения запроса.

Пример

Запрос:

```
POST https://localhost/api/v1/analysis/listTasks
```

Ответ:

```
{
  "next_cursor": "",
  "tasks": [
    {
      "duration": 2.063644,
      "duration_full": 2.864644,
      "entry_point_id": "tw-1206-c",
      "entry_point_type": "PUBLIC_API",
      "id": "b4924f52-1074-11f0-8448-ced2d2aff785",
      "name": "",
      "scan_state": "FULL",
      "start_time": 1743675388.02236,
      "threat": "UNKNOWN",
      "verdict": "CLEAN"
    },
    {
      "duration": 2.373042,
      "duration_full": 2.851042,
      "entry_point_id": "tw-1206-c",
      "entry_point_type": "PUBLIC_API",
      "id": "7736256e-106e-11f0-83f2-ced2d2aff785",
      "name": "",
      "scan_state": "FULL",
      "start_time": 1743672708.09696,
      "threat": "HACKTOOL",
      "verdict": "DANGEROUS"
    }
  ]
}
```

2.5. Скачивание файла из хранилища

Ваше приложение может скачать файл из PT Email Security.

Метод и URL запроса:

POST <Корневой URL API>/storage/downloadArtifact

Тело запроса должно содержать параметр `file_uri`. В качестве значения параметра должны быть указаны название алгоритма, по которому была вычислена хеш-сумма файла — `sha256`, двоеточие и сама хеш-сумма.

Примечание. Ваше приложение может получить значение для параметра `file_uri` из ответа на [запрос проверки файла \(см. раздел 2.2.2\)](#). В этом случае URI файла в нужном формате можно взять из поля `data` → `artifacts` → `file_info` → `file_uri`.

Ответ на запрос

В ответ на корректно составленный запрос публичный API присылает сообщение с кодом 200. В теле этого сообщения — запрошенный файл в бинарном виде (MIME-тип — application/octet-stream).

В ответ на неуспешный запрос сервис публичного API присылает сообщение с кодом ошибки. Тело такого сообщения содержит поля, описанные [по схеме ответа на неуспешный запрос \(см. раздел 2.8.2\)](#).

Возможные коды ошибок и их значения:

- 400 — запрос составлен неверно (например, нет параметра `file_uri`);
- 401 — в запросе нет токена доступа или он указан неверно;
- 404 — файл с указанной хеш-суммой не найден в PT Email Security;
- 405 — неправильно указан метод запроса.

Пример

Тело запроса:

```
{ "file_uri":
  "sha256:32E7802D1E4723F2A529F199EDF62EF74A21640DE379250ECFB7D5C17A2D5A0" }
```

Ответ, когда запрос был составлен неверно:

```
{
  "data": {},
  "errors": [
    {
      "message": "{\'file_uri\': [\'Missing data for required field.\']}",
      "type": "HTTPBadRequest"
    }
  ]
}
```

2.6. Получение информации об образах виртуальных машин

Ваше приложение может получить список образов виртуальных машин, установленных в PT Email Security.

Метод и URL запроса:

```
POST <Корневой URL API>/engines/sandbox/getImages
```

Параметры запроса отсутствуют.

Ответ на запрос

В ответ на успешный запрос сервис публичного API присылает сообщение с кодом 200. Тело ответного сообщения может содержать поля, описанные в таблице ниже.

Таблица 11. Поля в ответном сообщении на запрос образов виртуальных машин

Поле	Тип	Описание
data	Array of JSON objects	Информация об образах виртуальных машин. Каждый образ описывается в виде JSON-объекта по схеме image (см. раздел 2.8.3)
errors	Array of JSON objects	Не заполняется

Возможные коды ошибок и их значения:

- 401 — в запросе нет токена доступа или он указан неверно;
- 405 — неправильно указан метод запроса.

Пример

Запрос:

```
POST /api/v1/engines/sandbox/getImages
```

Ответ на успешный запрос:

```
{
  "data": [
    {
      "image_id": "win10-1803-x64",
      "version": "55",
      "os": {
        "name": "Windows 10 Pro",
        "version": "10.0.17134",
        "architecture": "x64",
        "service_pack": "",
        "locale": "en-US"
      }
    },
    {
      "image_id": "win7-sp1-x64",
      "version": "78",
      "os": {
        "name": "Windows 7 ENTERPRISE",
        "version": "6.1.7601",
        "architecture": "x64",
        "service_pack": "Service Pack 1",

```

```

        "locale": "en-US"
      }
    ],
    "errors": []
  }

```

Ответ на неуспешный запрос:

```

{
  "data": {},
  "errors": [
    {
      "message": "405: Method Not Allowed",
      "type": "HTTPMethodNotAllowed"
    }
  ]
}

```

2.7. Получение состояния API

Ваше приложение может получить текущее состояние публичного API.

Примечание. Запрос может быть отправлен методами POST и GET.

Метод и URL запроса:

POST <Корневой URL API>/maintenance/checkHealth

Параметры запроса отсутствуют.

Ответ на запрос

В ответ на успешный запрос сервис публичного API присылает сообщение с кодом 200. Тело ответного сообщения может содержать поля, описанные в таблице ниже.

Таблица 12. Поля в ответе на запрос состояния публичного API

Поле	Тип	Описание
data → status	String	Состояние работы сервиса публичного API. Возможное значение — OK. При наличии ошибки отсутствует
errors	Array of JSON objects	Не заполняется

В ответ на неуспешный запрос сервис публичного API присылает сообщение с кодом ошибки. Тело такого сообщения содержит поля, описанные [по схеме ответа на неуспешный запрос \(см. раздел 2.8.2\)](#).

Возможные коды ошибок и их значения:

- 401 — в запросе нет токена доступа или он указан неверно;
- 403 — недействительная лицензия или для переданного в запросе токена доступа среди разрешенных действий нет необходимого для выполнения запроса.

Пример

Запрос:

```
POST /maintenance/checkHealth
```

Ответ на успешный запрос:

```
{
  "data": {
    "status": "OK"
  },
  "errors": []
}
```

Ответ на неуспешный запрос:

```
{
  "data": {},
  "errors": [
    {
      "message": "405: Method Not Allowed",
      "type": "HTTPMethodNotAllowed"
    }
  ]
}
```

2.8. Описание схем данных

В этом разделе приведены схемы данных, используемые в ответах на запросы к публичному API.

В этом разделе

[Схема ответа с результатами проверки \(см. раздел 2.8.1\)](#)

[Схема ответа на неуспешный запрос \(см. раздел 2.8.2\)](#)

[Схема image \(см. раздел 2.8.3\)](#)

[Схема os \(см. раздел 2.8.4\)](#)

2.8.1. Схема ответа с результатами проверки

Описывает ответ на запрос на проверку файла или на получение результатов проверки файла.

Таблица 13. Поля с результатами проверки

Поле	Тип	Описание
data → scan_id	String	Идентификатор задания на проверку. Примечание. Используя идентификатор задания, вы можете просмотреть результаты проверки в веб-интерфейсе по ссылке <a href="https://<Адрес PT Email Security>/#/events/shared/<Идентификатор задания на проверку>">https://<Адрес PT Email Security>/#/events/shared/<Идентификатор задания на проверку>
data → result	JSON object	Общий результат проверки по схеме result (см. раздел 2.8.1.1). Отсутствует в ответах на запросы: — createScanTask с включенным параметром async_result; — createScanURLTask с включенным параметром async_result; — checkTask, если проверка файла еще не завершена; — report, если проверка файла еще не завершена; — scan/checkFile с включенным параметром async_result; — scan/checkURL с включенным параметром async_result; — scan/getStatus, если проверка файла еще не завершена; — scan/getFullReport, если проверка файла еще не завершена
data → artifacts	Array of JSON objects	Файлы, электронные письма или другие объекты, которые были проверены в ходе проверки файла, URI которого был указан в запросе createScanTask, или в ходе проверки ссылок через запросы scan/checkURL и

Поле	Тип	Описание
		createScanURLTask. Каждый проверенный объект описывается в виде JSON-объекта по схеме artifact (см. раздел 2.8.1.2). Отсутствует в ответах на запросы: — createScanTask с включенным параметром <code>async_result</code> или <code>short_result</code>; — createScanURLTask с включенным параметром <code>async_result</code> или <code>short_result</code>; — checkTask; — scan/checkFile с включенным параметром <code>async_result</code> или <code>short_result</code>; — scan/checkURL с включенным параметром <code>async_result</code> или <code>short_result</code>; — scan/getStatus
errors	Array of JSON objects	Не заполняется

В этом разделе

[Схема result \(см. раздел 2.8.1.1\)](#)

[Схема artifact \(см. раздел 2.8.1.2\)](#)

[Схема file_info \(см. раздел 2.8.1.3\)](#)

[Схема download_url_info \(см. раздел 2.8.1.4\)](#)

[Схема engine_result \(см. раздел 2.8.1.5\)](#)

[Схема log \(см. раздел 2.8.1.6\)](#)

[Схема network_object \(см. раздел 2.8.1.7\)](#)

[Схема error \(см. раздел 2.8.1.8\)](#)

2.8.1.1. Схема result

Описывает результат проверки.

Таблица 14. Поля в схеме result

Поле	Тип	Описание
scan_state	String	Статус проверки. Возможные значения: — <code>PARTIAL</code> — частичная проверка; — <code>FULL</code> — полная проверка; — <code>UNSCANNED</code> — проверка не проведена
duration	Float	Длительность проверки в секундах. Записывается только в общих результатах проверки (в JSON-объекте <code>data</code> → <code>result</code>). Отсутствует в ответе на запрос <code>checkTask</code> с результатами проверки, запущенной асинхронным запросом <code>createScanTask</code> (с включенным параметром <code>async_result</code>)
verdict	String	Результат проверки. Возможные значения: — <code>CLEAN</code> — угроз не обнаружено; — <code>UNWANTED</code> — потенциально опасный; — <code>DANGEROUS</code> — опасный
threat	String	Тип обнаруженного вредоносного ПО
errors	Array of JSON objects	Ошибки, возникшие в ходе проверки. Присутствует только в JSON-объекте <code>data</code> → <code>artifacts[]</code> → <code>result</code> . Каждая ошибка описывается в виде JSON-объекта по схеме error (см. раздел 2.8.1.8)

2.8.1.2. Схема artifact

Описывает проверяемый файл.

Таблица 15. Поля в схеме artifact

Поле	Тип	Описание
type	String	Тип проверенного объекта. Возможные значения: — <code>FILE</code> — обычный файл; — <code>ARCHIVE</code> — архив; — <code>COMPRESSED</code> — сжатый файл; — <code>EMAIL</code> — электронное письмо

Поле	Тип	Описание
result	JSON object	Результат проверки файла по схеме result (см. раздел 2.8.1.1)
file_info	JSON object	Информация о проверенном файле по схеме file_info (см. раздел 2.8.1.3)
download_url_info	JSON object	Информация о проверенной ссылке по схеме download_url_info (см. раздел 2.8.1.4)
engine_results	Array of JSON objects	Результаты проверки файла конкретными антивирусами или другими компонентами. Каждый результат описывается в JSON-объекте по схеме engine_result (см. раздел 2.8.1.5)
artifacts	Array of JSON objects	Файлы, упакованные в архив. Если отправленный на проверку файл не является архивом или превышена допустимая глубина распаковки, массив <code>artifacts</code> будет пустым. Каждый файл в этом массиве описывается в виде JSON-объекта по схеме artifact (см. раздел 2.8.1.2)
network_objects	Array of JSON objects	Информация о сетевых объектах выполненного задания. Каждый сетевой объект описывается в виде JSON-объекта по схеме network_object (см. раздел 2.8.1.7)

См. также

[Схема engine_result](#) (см. раздел 2.8.1.5)

[Схема artifact](#) (см. раздел 2.8.1.2)

2.8.1.3. Схема file_info

Описывает свойства файла.

Таблица 16. Поля в схеме file_info

Поле	Тип	Описание
file_uri	String	Идентификатор файла. Может использоваться для его скачивания (см. раздел 2.5)
file_path	String	Путь к файлу (исключая корневой файл структуры), включая его название. Например, для файла <code>readme.txt</code> в корне архива

Поле	Тип	Описание
		<code>archive.zip</code> в качестве значения этого поля будет указано <code>readme.txt</code> , для самого архива — пустое значение
<code>mime_type</code>	String	MIME-тип файла, определенный в процессе проверки
<code>md5</code>	String	MD5-хеш-сумма файла
<code>sha1</code>	String	SHA-1-хеш-сумма файла
<code>sha256</code>	String	SHA-256-хеш-сумма файла
<code>ssdeep</code>	String	SSDEEP-хеш-сумма файла
<code>size</code>	Integer	Размер файла в байтах

2.8.1.4. Схема `download_url_info`

Описывает свойства проверенной ссылки.

Таблица 17. Поля в схеме `download_url_info`

Поле	Тип	Описание
<code>reason_phrase</code>	String	Описание кода ответа на HTTP-запрос (Reason-Phrase)
<code>state</code>	String	Статус проверки ссылки. Возможные значения: — <code>FULL</code> — проверка выполнена полностью; — <code>PARTIAL</code> — выполнена частично; — <code>UNSCANNED</code> — не выполнена; — <code>UNKNOWN</code> — статус неизвестен
<code>status_code</code>	Integer	Код ответа на HTTP-запрос
<code>version</code>	String	Версия CMS

2.8.1.5. Схема `engine_result`

Описывает результат проверки конкретным антивирусом или другим проверяющим компонентом.

Таблица 18. Поля в схеме engine_result

Поле	Тип	Описание
engine_subsystem	String	Метод проверки. Возможные значения: — AV — антивирусное сканирование; — SANDBOX — поведенческий анализ; — STATIC — экспертная оценка файлов
engine_code_name	String	Название антивируса или компонента
engine_version	String	Версия антивируса или компонента
database_version	String	Версия антивирусной базы или базы знаний
database_time	Float	Время обновления антивирусной базы или базы знаний
result	JSON object	Результат проверки антивирусом или другим компонентом по схеме result (см. раздел 2.8.1.1)
detections	Array of JSON objects	Описание обнаруженного вредоносного ПО
detections → detect	String	Вредоносное ПО
detections → threat	String	Тип вредоносного ПО
details → sandbox	JSON object	Подробная информация о поведенческом анализе (если проводился)
details → sandbox → image	JSON object	Информация об образе виртуальной машины по схеме image (см. раздел 2.8.3)
details → sandbox → logs	Array of JSON objects	Копия сетевого трафика, видеозапись, журналы событий. Каждый объект описывается по схеме log (см. раздел 2.8.1.6)
details → sandbox → artifacts	Array of JSON objects	Артефакты виртуальной машины — файлы, созданные в ходе поведенческого анализа. Каждый файл описывается в виде JSON-объекта по схеме artifact (см. раздел 2.8.1.2)
details → sandbox → network_objects	Array of JSON objects	Информация о сетевых объектах выполненного задания. Каждый сетевой объект описывается в виде JSON-объекта по схеме network_object (см. раздел 2.8.1.7)

2.8.1.6. Схема log

Описывает файлы, созданные для поведенческого анализа: копию сетевого трафика, видеозаписи и журналы событий.

Таблица 19. Поля в схеме log

Поле	Тип	Описание
type	String	Тип созданного файла. Возможные значения: — <code>NETWORK</code> — копия сетевого трафика в формате PCAP; — <code>SCREENSHOT</code> — снимок или видеозапись экрана виртуальной машины; — <code>EVENT_RAW</code> — необработанный список событий в простом текстовом формате; — <code>EVENT_CORRELATED</code> — нормализованные события, проанализированные с помощью правил корреляции для нахождения закономерностей и выявления опасного и потенциально опасного поведения (в формате JSON); — <code>EVENT_NORMALIZED</code> — события, приведенные к единому виду, пригодному для дальнейшего анализа (в формате JSON);
file_uri	String	Идентификатор файла. Используется для скачивания
file_name	String	Название файла

2.8.1.7. Схема network_object

Описывает сетевые объекты выполненного задания.

Таблица 20. Поля в схеме network_object

Поле	Тип	Описание
type	String	Тип сетевого объекта. Возможные значения: — <code>DOMAIN</code> — доменное имя; — <code>IP</code> — IP-адрес; — <code>URL</code> — URL-адрес

Поле	Тип	Описание
value	String	Значение сетевого объекта

2.8.1.8. Схема error

Описывает ошибки, возникающие в ходе выполнения проверки.

Таблица 21. Поля в схеме error

Поле	Тип	Описание
message	String	Сообщение об ошибке
type	String	Тип ошибок: — <code>corrupted</code> — получен поврежденный объект, например поврежденный архив; — <code>encrypted</code> — не удалось распаковать или проверить зашифрованный объект; — <code>internal</code> — внутренняя ошибка средства проверки; — <code>max_depth_exceeded</code> — превышен допустимый уровень вложенности архива; — <code>sandbox_run_sample</code> — не удалось выполнить поведенческий анализ файла

2.8.2. Схема ответа на неуспешный запрос

В ответ на неуспешный запрос сервис публичного API присылает сообщение с кодом ошибки. Тело такого сообщения содержит описание ошибок, возникших в ходе выполнения запроса.

Тело ответа:

```
{
  "data": {
  },
  "errors": [
    <JSON object 1>,
    <JSON object 2>,
    ...
  ]
}
```

Тело ответа содержит поля, описанные в таблице.

Таблица 22. Поля в теле ответа на неуспешный запрос

Поле	Тип	Описание
data	JSON object	Не заполняется
errors	Array of JSON objects	Информация об ошибках
errors → <JSON object>		
<pre>{ "message": "<String>", "type": "<String>" }</pre>		
message	String	Сообщение об ошибке. Для ошибки 401 возвращается значение <code>Authorization required</code> (требуется авторизация). Для ошибки 403 возвращаются значения: — <code>Forbidden</code> — доступ запрещен; — <code>No license</code> — нет лицензии; — <code>Bad license</code> — недействительная лицензия. Для других ошибок не заполняется
type	String	Тип ошибки. Для ошибки 401 возвращается значение <code>HTTPUnauthorized</code> (неавторизованный доступ). Для ошибки 403 возвращается значение <code>HTTPForbidden</code> (доступ запрещен). Для других ошибок не заполняется

Пример

Ответ на неуспешный запрос:

```
{
  "data": {
  },
  "errors": [
    {
      "message": "403: Forbidden",
      "type": "HTTPForbidden"
    }
  ]
}
```

2.8.3. Схема image

Описывает образ виртуальной машины.

Таблица 23. Поля в схеме image

Поле	Тип	Описание
image_id	String	Идентификатор образа виртуальной машины
version	String	Версия образа виртуальной машины
os	JSON object	Информация об операционной системе образа виртуальной машины по схеме os (см. раздел 2.8.4)

2.8.4. Схема os

Описывает операционную систему образа виртуальной машины.

Таблица 24. Поля в схеме os

Поле	Тип	Описание
name	String	Название операционной системы
version	String	Версия операционной системы
architecture	String	Архитектура процессора, которую поддерживает операционная система
service_pack	String	Название пакета обновления операционной системы
locale	String	Локаль операционной системы

3. Формат сообщений syslog

Сообщения стандарта syslog могут использоваться для централизованного сбора и анализа событий ИБ в информационной системе вашей организации. Включить и настроить отправку таких сообщений на внешний syslog-сервер вы можете через веб-интерфейс PT Email Security. При этом будут отправляться сообщения о новых объектах, о начале и окончании работы с источниками объектов, о результатах проверки объектов средствами проверки, о вердиктах по объектам и по заданиям. Также отправляются сообщения об обновлении средств проверки и их баз. Все сообщения соответствуют стандарту [RFC 5424](#) и имеют следующий вид:

```
<100>1 <Дата и время сообщения> <Имя узла PT Email Security> emailsecurity - <Тип сообщения> - <Тело сообщения JSON>
```

В заголовке для всех сообщений указываются приоритет 100, версия 1, дата и время получения syslog-сервером, имя основного узла PT Email Security, метка emailsecurity и тип сообщения MSGID. Тело сообщения в формате JSON содержит основную информацию, а его структура зависит от типа сообщения.

В этом разделе

[Порядок отправки сообщений \(см. раздел 3.1\)](#)

[Типы данных полей \(см. раздел 3.2\)](#)

[Начало работы с источником \(см. раздел 3.3\)](#)

[Добавление объекта, new_artifact \(см. раздел 3.4\)](#)

[Проверка объекта \(см. раздел 3.5\)](#)

[Завершение работы с источником \(см. раздел 3.6\)](#)

[Обновление средства проверки, av.update \(см. раздел 3.7\)](#)

[События аудита, audit.event \(см. раздел 3.8\)](#)

[Типы источников \(см. раздел 3.9\)](#)

[Средства проверки \(см. раздел 3.10\)](#)

[Типы вредоносного ПО \(см. раздел 3.11\)](#)

3.1. Порядок отправки сообщений

В процессе работы PT Email Security отправляются следующие сообщения syslog:

1. При поступлении объекта от источника создается задание на проверку объекта — отправляется сообщение о начале работы с источником <Тип источника>.start.
2. Для поступившего на проверку объекта отправляется сообщение new_artifact. Если из объекта выделяются дочерние объекты, то для каждого такого объекта также отправляется сообщение new_artifact. Все сообщения, отправляемые для дочерних объектов, содержат информацию о родительском объекте, это позволяет составить иерархию объектов.

3. Каждый объект, для которого отправлено сообщение `new_artifact`, отправляется на проверку:

- Если в процессе проверки из объекта извлекаются дочерние объекты (например, файлы из архива, письма или ISO-файла), для каждого дочернего объекта отправляется сообщение `scan_machine.new_object` и `new_artifact` (с информацией о родительском объекте). Извлеченные объекты также отправляются на проверку.
- Объект проверяется средствами проверки в соответствии с заданными в задании параметрам проверки. Для каждого средства проверки отправляется сообщение с результатами проверки `scan_machine.file_result.av`.
- Если в параметрах проверки настроена проверка методом поведенческого анализа, по его завершении отправляется сообщение `scan_machine.file_result.pt_sandbox`.

Если в ходе поведенческого анализа появляются артефакты (например, дампы памяти, файлы, создаваемые проверяемым приложением), для каждого из них отправляется сообщение `new_artifact` (с информацией о родительском объекте). Все артефакты отправляются на проверку.

- По каждому объекту задания выносится вердикт и отправляется сообщение `scan_machine.file_result.melded`. Вердикт выносится на основании результатов проверок объекта всеми средствами проверки и вердиктов дочерних объектов.

4. По заданию выносится вердикт — отправляется сообщение `scan_machine.final_result`. Вердикт выносится на основании вердикта исходного объекта задания и вердиктов дочерних объектов.

5. По завершении задания принимается решение о блокировке объекта задания и отправляется сообщение о завершении работы с источником `<Тип источника>.finish`.

Если объект поступил на проверку от источника, работающего в пассивном режиме, сообщение о завершении работы с источником `<Тип источника>.finish` может быть отправлено раньше сообщения о завершении проверки `scan_machine.final_result`.

Кроме того, при каждом обновлении средств проверки и их баз отправляется сообщение `av.update`.

3.2. Типы данных полей

В таблице указаны типы данных, которые используются для полей сообщений.

Таблица 25. Типы данных полей

Тип	Назначение	Пример
Boolean	Логическое значение	true, false
Enum	Один из элементов предопределенного списка значений с типом данных String	DANGEROUS
Float	Число с плавающей точкой (занимает 64 бита)	1511421763.3728465

Тип	Назначение	Пример
String	Строка. Значение нужно указывать в кавычках	"archive.zip"
UInt32	Целое число от 0 до 4 294 967 295 (занимает 32 бита)	534333
UInt64	Целое число от 0 до 18 446 744 073 709 551 615 (занимает 64 бита)	5664000000
UUID	128-битный (16-байтный) идентификатор, представленный в виде строки из 36 символов в формате RFC 4122	123e4567-e89b-12d3-a456-426655440000

3.3. Начало работы с источником

При поступлении объекта от источника PT Email Security создает задание на проверку и отправляется сообщение о начале работы с источником. В разделе описаны типы сообщений, которые отправляются для указанных в таблице источников.

Таблица 26. Типы сообщений, отправляемые при начале работы с источниками

Тип сообщения	Источник
user_scan.start	Веб-интерфейс
check_me.start	Служба Checkme
email.start	Сервер Microsoft Exchange с установленным агентом
mail_agent_mta.start	Почтовый шлюз безопасности
mail_bcc.start	Почтовый сервер в режиме зеркалирования
mail_gateway.start	Почтовый сервер в режиме фильтрации
mail_gateway_mta.start	Почтовый сервер в режиме фильтрации (MTA)
files_monitor.start	Общая папка
files_inbox.start	Папка-шлюз
icap.start	ICAP-сервер
dpi.start	PT NAD
pt_edr.start	MaxPatrol EDR
retro.start	Хранилище файлов (при запуске повторной проверки файлов)
public_api.start	Публичный API при проверке с передаваемыми параметрами
scan_api.start	Публичный API при проверке с параметрами источника

В этом разделе

- [Сообщение user_scan.start \(см. раздел 3.3.1\)](#)
- [Сообщение check_me.start \(см. раздел 3.3.2\)](#)
- [Сообщение email.start \(см. раздел 3.3.3\)](#)
- [Сообщение mail_agent_mta.start \(см. раздел 3.3.4\)](#)
- [Сообщение mail_bcc.start \(см. раздел 3.3.5\)](#)
- [Сообщение mail_gateway.start \(см. раздел 3.3.6\)](#)
- [Сообщение mail_gateway_mta.start \(см. раздел 3.3.7\)](#)
- [Сообщение files_monitor.start \(см. раздел 3.3.8\)](#)
- [Сообщение files_inbox.start \(см. раздел 3.3.9\)](#)
- [Сообщение icap.start \(см. раздел 3.3.10\)](#)
- [Сообщение dpi.start \(см. раздел 3.3.11\)](#)
- [Сообщение retro.start \(см. раздел 3.3.12\)](#)
- [Сообщение public_api.start \(см. раздел 3.3.13\)](#)
- [Сообщение scan_api.start \(см. раздел 3.3.14\)](#)
- [Сообщение pt_edr.start \(см. раздел 3.3.15\)](#)

3.3.1. Сообщение user_scan.start

Сообщение отправляется при получении объекта через веб-интерфейс.

Тело сообщения:

```
{
  "scan_id": "<String>",
  "created": <Float>,
  "received": <Float>,
  "http": <JSON object>,
  "user": <JSON object>
}
```

Таблица 27. Поля сообщения user_scan.start

Поле (объект)	Тип данных	Описание
scan_id	String	Идентификатор задания на проверку
created	Float	UNIX-время создания сообщения
received	Float	UNIX-время создания задания на проверку

Поле (объект)	Тип данных	Описание
http	JSON object	Информация об HTTP-запросе браузера при загрузке объекта
user	JSON object	Информация о пользователе, загрузившем объект
http		
<pre>{ "client_ip": "<String>", "user_agent": "<String>" }</pre>		
client_ip	String	IP-адрес клиента, с помощью которого был осуществлен запрос
user_agent	String	Название и версия браузера
user		
<pre>{ "id": <UInt32>, "login": "<String>", "name": "<String>" }</pre>		
id	UInt32	Идентификатор пользователя в продукте
login	String	Логин пользователя
name	String	Фамилия, имя и отчество пользователя

Примеры

Пример сообщения при начале работы с источником:

```
<100>1 2024-01-15T07:22:44.018041Z example-host emailsecurity - user_scan.start - {
  "scan_id": "a36a1f7c-51af-32b1-a144-659b1dfe31c1",
  "received": 1511421762.957363,
  "created": 1511421763.3728465,
  "user": {
    "id": 534333,
    "name": "Ivan Ivanov",
    "login": "username"
  },
  "http": {
    "client_ip": "192.0.2.32",
    "user_agent": "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
    Gecko) Chrome/51.0.2704.103 Safari/537.36"
  }
}
```

3.3.2. Сообщение check_me.start

Сообщение отправляется при получении службой Checkme письма на проверку.

Тело сообщения:

```
{
  "scan_id": "<String>",
  "created": <Float>,
  "received": <Float>,
  "entry_point_id": "<String>",
  "envelope": <JSON-object>,
  "email": <JSON-object>
}
```

Таблица 28. Поля сообщения check_me.start

Поле (объект)	Тип данных	Описание
scan_id	String	Идентификатор задания на проверку
created	Float	UNIX-время создания сообщения
received	Float	UNIX-время создания задания на проверку
entry_point_id	String	Название источника для проверки, указанное в веб-интерфейсе
envelope	JSON object	Данные из поля Envelope электронного письма
email	JSON object	Информация о письме

envelope		
<pre>{ "from_address": "<String>", "recipients": ["<String>"] }</pre>		
from_address	String	Адрес электронной почты отправителя письма
recipients	Array of strings	Данные о получателях письма

Поле (объект)	Тип данных	Описание
email		
<pre>{ "id": "<String>", "references": "<String>", "reply_to": "<String>", "subject": "<String>", "from_address": { "address": "<String>", "name": "<String>" }, "to": { "address": "<String>", "name": "<String>" }, "to_list": [{ "address": "<String>", "name": "<String>" }], "cc": { "address": "<String>", "name": "<String>" }, "cc_list": [{ "address": "<String>", "name": "<String>" }], "bcc": { "address": "<String>", "name": "<String>" }, "bcc_list": [{ "address": "<String>", "name": "<String>" }], }</pre>		
id	String	Поле заголовка Message-ID

Поле (объект)	Тип данных	Описание
references	String	Идентификационное поле заголовка references согласно RFC 5322
reply_to	String	Идентификационное поле заголовка in-reply-to согласно RFC 5322
subject	String	Тема письма
address	String	Адрес электронной почты
from_address	JSON object	Информация об отправителе письма
<Адресное поле> → address	String	Адрес электронной почты отправителя (получателя) письма
<Адресное поле> → name	String	Имя отправителя (получателя) письма
to	JSON object	Информация о получателе письма (первом из списка)
to_list	Array of JSON objects	Информация о получателях письма
cc	JSON object	Информация о получателе копии письма (первом из списка)
cc_list	Array of JSON objects	Информация о получателях копии письма
bcc	JSON object	Информация о получателе скрытой копии письма (первом из списка)
bcc_list	Array of JSON objects	Информация о получателях скрытой копии письма

Примеры

Пример сообщения при начале работы с источником:

```
<100>1 2024-01-15T07:22:44.018041Z example-host emailsecurity - check_me.start - {
  "scan_id": "a36a1f7c-51af-32b1-a144-659b1dfe31c1",
  "created": 1511421763.3728465,
  "received": 1511421762.957363,
  "entry_point_id": "checkme-service",
  "envelope": {
    "from_address": "ivanov@example.org",
    "recipients": ["checkme@example.org", "username@example.org",
"username23@example.net", "admin@example.org"]
  },
  "email": {
    "id": "<6fee62f024e0@example.com>",
    "subject": "Проверка файла",
    "references": "user@example.org",
    "reply_to": "",
    "from_address": {
      "address": "ivanov@example.org",
      "name": "Ivan Ivanov"
    },
    "to": {
      "address": "checkme@example.org",
      "name": ""
    },
    "to_list": [
      {
        "address": "checkme@example.org",
        "name": ""
      }
    ],
    "cc": {
      "address": "username_12@example.org",
      "name": "Ivan Ivanov"
    },
    "cc_list": [
      {
        "address": "username_12@example.org",
        "name": "Ivan Ivanov"
      },
      {
        "address": "username23@example.net",
        "name": ""
      }
    ],
  },
}
```

```

    "bcc": {
      "address": "admin@example.org",
      "name": ""
    },
    "bcc_list": [
      {
        "address": "admin@example.org",
        "name": ""
      }
    ]
  }
}

```

3.3.3. Сообщение email.start

Сообщение отправляется при получении почтовым агентом письма на проверку.

Тело сообщения:

```

{
  "scan_id": "<String>",
  "created": <Float>,
  "received": <Float>,
  "entry_point_id": "<String>",
  "envelope": <JSON object>,
  "email": <JSON object>
}

```

Таблица 29. Поля сообщения email.start

Поле (объект)	Тип данных	Описание
scan_id	String	Идентификатор задания на проверку
created	Float	UNIX-время создания сообщения
received	Float	UNIX-время создания задания на проверку
entry_point_id	String	Название источника для проверки, указанное в веб-интерфейсе
envelope	JSON object	Данные из поля Envelope электронного письма
email	JSON object	Информация о письме

Поле (объект)	Тип данных	Описание
envelope		
<pre>{ "from_address": "<String>", "recipients": ["<String>"] }</pre>		
from_address	String	Адрес электронной почты отправителя письма
recipients	Array of strings	Данные о получателях письма

Поле (объект)	Тип данных	Описание
email		
<pre>{ "id": "<String>", "references": "<String>", "reply_to": "<String>", "subject": "<String>", "from_address": { "address": "<String>", "name": "<String>" }, "to": { "address": "<String>", "name": "<String>" }, "to_list": [{ "address": "<String>", "name": "<String>" }], "cc": { "address": "<String>", "name": "<String>" }, "cc_list": [{ "address": "<String>", "name": "<String>" }], "bcc": { "address": "<String>", "name": "<String>" }, "bcc_list": [{ "address": "<String>", "name": "<String>" }], }</pre>		
id	String	Поле заголовка Message-ID

Поле (объект)	Тип данных	Описание
references	String	Идентификационное поле заголовка references согласно RFC 5322
reply_to	String	Идентификационное поле заголовка in-reply-to согласно RFC 5322
subject	String	Тема письма
address	String	Адрес электронной почты
from_address	JSON object	Информация об отправителе письма
<Адресное поле> → address	String	Адрес электронной почты отправителя (получателя) письма
<Адресное поле> → name	String	Имя отправителя (получателя) письма
to	JSON object	Информация о получателе письма (первом из списка)
to_list	Array of JSON objects	Информация о получателях письма
cc	JSON object	Информация о получателе копии письма (первом из списка)
cc_list	Array of JSON objects	Информация о получателях копии письма
bcc	JSON object	Информация о получателе скрытой копии письма (первом из списка)
bcc_list	Array of JSON objects	Информация о получателях скрытой копии письма

Примеры

Пример сообщения при начале работы с источником:

```
<100>1 2024-01-15T07:22:44.018041Z example-host emailsecurity - email.start - {
  "scan_id": "a36a1f7c-51af-32b1-a144-659b1dfe31c1",
  "created": 1511421763.37285,
  "received": 1511421762.95736,
  "entry_point_id": "mail-agent",
  "envelope": {
    "from_address": "ivanov@example.org"
  },
  "email": {
    "id": "<6fee62f024e0@example.com>",
    "references": "",
    "reply_to": "",
    "subject": "Последняя версия моей программы",
    "from_address": {
      "address": "ivanov@example.org",
      "name": "Ivan Ivanov"
    },
    "to": {
      "address": "username@example.com",
      "name": "Ivan Ivanov"
    },
    "to_list": [
      {
        "address": "username@example.com",
        "name": "Ivan Ivanov"
      }
    ],
    "cc": {
      "address": "username_12@example.org",
      "name": "Ivan Ivanov"
    },
    "cc_list": [
      {
        "address": "username_12@example.org",
        "name": "Ivan Ivanov"
      },
      {
        "address": "username23@example.net",
        "name": ""
      }
    ],
    "bcc": {
      "address": "admin@example.org",
```



```

        "name": ""
    },
    "bcc_list": [
        {
            "address": "admin@example.org",
            "name": ""
        }
    ]
}

```

3.3.4. Сообщение mail_agent_mta.start

Сообщение отправляется при получении письма от почтового шлюза безопасности.

Тело сообщения:

```

{
    "scan_id": "<String>",
    "created": <Float>,
    "received": <Float>,
    "entry_point_id": "<String>",
    "client": <JSON object>,
    "envelope": <JSON object>,
    "email": <JSON object>
}

```

Таблица 30. Поля сообщения mail_agent_mta.start

Поле (объект)	Тип данных	Описание
scan_id	String	Идентификатор задания на проверку
created	Float	UNIX-время создания сообщения
received	Float	UNIX-время создания задания на проверку
entry_point_id	String	Название источника для проверки, указанное в веб-интерфейсе
client	JSON object	Информация об SMTP-клиенте
envelope	JSON object	Данные из поля Envelope электронного письма
email	JSON object	Информация о письме

Поле (объект)	Тип данных	Описание
client		
<pre>{ "address": "<String>", "ip": "<String>", "port": <UInt32> }</pre>		
address	String	IP-адрес SMTP-клиента
ip	String	IP-адрес SMTP-клиента
port	UInt32	Порт SMTP-клиента
envelope		
<pre>{ "from_address": "<String>", "recipients": ["<String>"] }</pre>		
from_address	String	Адрес электронной почты отправителя письма
recipients	Array of strings	Данные о получателях письма

Поле (объект)	Тип данных	Описание
email		
<pre>{ "id": "<String>", "references": "<String>", "reply_to": "<String>", "subject": "<String>", "from_address": { "address": "<String>", "name": "<String>" }, "to": { "address": "<String>", "name": "<String>" }, "to_list": [{ "address": "<String>", "name": "<String>" }], "cc": { "address": "<String>", "name": "<String>" }, "cc_list": [{ "address": "<String>", "name": "<String>" }], "bcc": { "address": "<String>", "name": "<String>" }, "bcc_list": [{ "address": "<String>", "name": "<String>" }], }</pre>		
id	String	Поле заголовка Message-ID

Поле (объект)	Тип данных	Описание
references	String	Идентификационное поле заголовка references согласно RFC 5322
reply_to	String	Идентификационное поле заголовка in-reply-to согласно RFC 5322
subject	String	Тема письма
address	String	Адрес электронной почты
from_address	JSON object	Информация об отправителе письма
<Адресное поле> → address	String	Адрес электронной почты отправителя (получателя) письма
<Адресное поле> → name	String	Имя отправителя (получателя) письма
to	JSON object	Информация о получателе письма (первом из списка)
to_list	Array of JSON objects	Информация о получателях письма
cc	JSON object	Информация о получателе копии письма (первом из списка)
cc_list	Array of JSON objects	Информация о получателях копии письма
bcc	JSON object	Информация о получателе скрытой копии письма (первом из списка)
bcc_list	Array of JSON objects	Информация о получателях скрытой копии письма

Примеры

Пример сообщения при начале работы с источником:

```
<100>1 2024-01-15T07:22:44.018041Z example-host emailsecurity - mail_agent_mta.start
- {
  "scan_id": "a36a1f7c-51af-32b1-a144-659b1dfe31c1",
  "created": 1511421763.3728465,
  "received": 1511421762.957363,
  "entry_point_id": "mail-gateway-mta",
  "client": {
    "ip": "203.0.113.33",
    "address": "203.0.113.33",
    "port": 36128
  },
  "envelope": {
    "from_address": "ivanov@example.org",
    "recipients": ["username@example.com"]
  },
  "email": {
    "id": "<6fee62f024e0@example.com>",
    "subject": "Последняя версия моей программы",
    "references": "",
    "reply_to": ""
    "from_address": {
      "address": "ivanov@example.org",
      "name": "Ivan Ivanov"
    },
    "to": {
      "address": "username@example.com",
      "name": "Ivan Ivanov"
    },
    "to_list": [
      {
        "address": "username@example.com",
        "name": "Ivan Ivanov"
      }
    ]
  }
}
```

3.3.5. Сообщение mail_bcc.start

Сообщение отправляется при получении письма от почтового сервера в виде скрытой копии.

Тело сообщения:

```
{
  "scan_id": "<String>",
  "created": <Float>,
  "received": <Float>,
  "entry_point_id": "<String>",
  "client": <JSON object>,
  "envelope": <JSON object>,
  "email": <JSON object>
}
```

Таблица 31. Поля сообщения mail_bcc.start

Поле (объект)	Тип данных	Описание
scan_id	String	Идентификатор задания на проверку
created	Float	UNIX-время создания сообщения
received	Float	UNIX-время создания задания на проверку
entry_point_id	String	Название источника для проверки, указанное в веб-интерфейсе
client	JSON object	Информация об SMTP-клиенте
envelope	JSON object	Данные из поля Envelope электронного письма
email	JSON object	Информация о письме
client		
<pre>{ "address": "<String>", "ip": "<String>", "port": <UInt32> }</pre>		
address	String	IP-адрес SMTP-клиента
ip	String	IP-адрес SMTP-клиента
port	UInt32	Порт SMTP-клиента
envelope		
<pre>{ "from_address": "<String>", "recipients": ["<String>"] }</pre>		

Поле (объект)	Тип данных	Описание
from_address	String	Адрес электронной почты отправителя письма
recipients	Array of strings	Данные о получателях письма

Поле (объект)	Тип данных	Описание
email		
<pre>{ "id": "<String>", "references": "<String>", "reply_to": "<String>", "subject": "<String>", "from_address": { "address": "<String>", "name": "<String>" }, "to": { "address": "<String>", "name": "<String>" }, "to_list": [{ "address": "<String>", "name": "<String>" }], "cc": { "address": "<String>", "name": "<String>" }, "cc_list": [{ "address": "<String>", "name": "<String>" }], "bcc": { "address": "<String>", "name": "<String>" }, "bcc_list": [{ "address": "<String>", "name": "<String>" }], }</pre>		
id	String	Поле заголовка Message-ID

Поле (объект)	Тип данных	Описание
references	String	Идентификационное поле заголовка references согласно RFC 5322
reply_to	String	Идентификационное поле заголовка in-reply-to согласно RFC 5322
subject	String	Тема письма
address	String	Адрес электронной почты
from_address	JSON object	Информация об отправителе письма
<Адресное поле> → address	String	Адрес электронной почты отправителя (получателя) письма
<Адресное поле> → name	String	Имя отправителя (получателя) письма
to	JSON object	Информация о получателе письма (первом из списка)
to_list	Array of JSON objects	Информация о получателях письма
cc	JSON object	Информация о получателе копии письма (первом из списка)
cc_list	Array of JSON objects	Информация о получателях копии письма
bcc	JSON object	Информация о получателе скрытой копии письма (первом из списка)
bcc_list	Array of JSON objects	Информация о получателях скрытой копии письма

Примеры

Пример сообщения при начале работы с источником:

```
<100>1 2024-01-15T07:22:44.018041Z example-host emailsecurity - mail_bcc.start - {
  "scan_id": "a36a1f7c-51af-32b1-a144-659b1dfe31c1",
  "created": 1511421763.37285,
  "received": 1511421762.95736,
  "entry_point_id": "mail-bcc",
  "client": {
    "address": "203.0.113.33",
    "ip": "203.0.113.33",
    "port": 36128
  },
  "envelope": {
    "from_address": "ivanov@example.org",
    "recipients": [
      "bcc@mailbox.local"
    ]
  },
  "email": {
    "id": "<6fee62f024e0@example.com>",
    "references": "",
    "reply_to": "",
    "subject": "Последняя версия моей программы",
    "from_address": {
      "address": "ivanov@example.org",
      "name": "Ivan Ivanov"
    },
    "to": {
      "address": "username@example.com",
      "name": "Ivan Ivanov"
    },
    "to_list": [
      {
        "address": "username@example.com",
        "name": "Ivan Ivanov"
      }
    ]
  }
}
```

3.3.6. Сообщение mail_gateway.start

Сообщение отправляется при получении письма от почтового сервера в режиме фильтрации.

Тело сообщения:

```
{
  "scan_id": "<String>",
  "created": <Float>,
  "received": <Float>,
  "entry_point_id": "<String>",
  "client": <JSON object>,
  "envelope": <JSON object>,
  "email": <JSON object>
}
```

Таблица 32. Поля сообщения mail_gateway.start

Поле (объект)	Тип данных	Описание
scan_id	String	Идентификатор задания на проверку
created	Float	UNIX-время создания сообщения
received	Float	UNIX-время создания задания на проверку
entry_point_id	String	Название источника для проверки, указанное в веб-интерфейсе
client	JSON object	Информация об SMTP-клиенте
envelope	JSON object	Данные из поля Envelope электронного письма
email	JSON object	Информация о письме
client		
<pre>{ "address": "<String>", "ip": "<String>", "port": <UInt32> }</pre>		
address	String	IP-адрес SMTP-клиента
ip	String	IP-адрес SMTP-клиента
port	UInt32	Порт SMTP-клиента
envelope		
<pre>{ "from_address": "<String>", "recipients": ["<String>"] }</pre>		

Поле (объект)	Тип данных	Описание
from_address	String	Адрес электронной почты отправителя письма
recipients	Array of strings	Данные о получателях письма

Поле (объект)	Тип данных	Описание
email		
<pre>{ "id": "<String>", "references": "<String>", "reply_to": "<String>", "subject": "<String>", "from_address": { "address": "<String>", "name": "<String>" }, "to": { "address": "<String>", "name": "<String>" }, "to_list": [{ "address": "<String>", "name": "<String>" }], "cc": { "address": "<String>", "name": "<String>" }, "cc_list": [{ "address": "<String>", "name": "<String>" }], "bcc": { "address": "<String>", "name": "<String>" }, "bcc_list": [{ "address": "<String>", "name": "<String>" }], }</pre>		
id	String	Поле заголовка Message-ID

Поле (объект)	Тип данных	Описание
references	String	Идентификационное поле заголовка references согласно RFC 5322
reply_to	String	Идентификационное поле заголовка in-reply-to согласно RFC 5322
subject	String	Тема письма
address	String	Адрес электронной почты
from_address	JSON object	Информация об отправителе письма
<Адресное поле> → address	String	Адрес электронной почты отправителя (получателя) письма
<Адресное поле> → name	String	Имя отправителя (получателя) письма
to	JSON object	Информация о получателе письма (первом из списка)
to_list	Array of JSON objects	Информация о получателях письма
cc	JSON object	Информация о получателе копии письма (первом из списка)
cc_list	Array of JSON objects	Информация о получателях копии письма
bcc	JSON object	Информация о получателе скрытой копии письма (первом из списка)
bcc_list	Array of JSON objects	Информация о получателях скрытой копии письма

Примеры

Пример сообщения при начале работы с источником:

```
<100>1 2024-01-15T07:22:44.018041Z example-host emailsecurity - mail_gateway.start -
{
  "scan_id": "a36a1f7c-51af-32b1-a144-659b1dfe31c1",
  "created": 1511421763.3728465,
  "received": 1511421762.957363,
  "entry_point_id": "mail-gateway",
  "client": {
    "ip": "203.0.113.33",
    "address": "203.0.113.33",
    "port": 36128
  },
  "envelope": {
    "from_address": "ivanov@example.org",
    "recipients": ["username@example.com"]
  },
  "email": {
    "id": "<6fee62f024e0@example.com>",
    "subject": "Последняя версия моей программы",
    "references": "",
    "reply_to": ""
    "from_address": {
      "address": "ivanov@example.org",
      "name": "Ivan Ivanov"
    },
    "to": {
      "address": "username@example.com",
      "name": "Ivan Ivanov"
    },
    "to_list": [
      {
        "address": "username@example.com",
        "name": "Ivan Ivanov"
      }
    ]
  }
}
```

3.3.7. Сообщение mail_gateway_mta.start

Сообщение отправляется при получении письма от почтового сервера в режиме фильтрации (MTA).

Тело сообщения:

```
{
  "scan_id": "<String>",
  "created": <Float>,
  "received": <Float>,
  "entry_point_id": "<String>",
  "client": <JSON object>,
  "envelope": <JSON object>,
  "email": <JSON object>
}
```

Таблица 33. Поля сообщения mail_gateway_mta.start

Поле (объект)	Тип данных	Описание
scan_id	String	Идентификатор задания на проверку
created	Float	UNIX-время создания сообщения
received	Float	UNIX-время создания задания на проверку
entry_point_id	String	Название источника для проверки, указанное в веб-интерфейсе
client	JSON object	Информация об SMTP-клиенте
envelope	JSON object	Данные из поля Envelope электронного письма
email	JSON object	Информация о письме
client		
<pre>{ "address": "<String>", "ip": "<String>", "port": <UInt32> }</pre>		
address	String	IP-адрес SMTP-клиента
ip	String	IP-адрес SMTP-клиента
port	UInt32	Порт SMTP-клиента
envelope		
<pre>{ "from_address": "<String>", "recipients": ["<String>"] }</pre>		

Поле (объект)	Тип данных	Описание
from_address	String	Адрес электронной почты отправителя письма
recipients	Array of strings	Данные о получателях письма

Поле (объект)	Тип данных	Описание
email		
<pre>{ "id": "<String>", "references": "<String>", "reply_to": "<String>", "subject": "<String>", "from_address": { "address": "<String>", "name": "<String>" }, "to": { "address": "<String>", "name": "<String>" }, "to_list": [{ "address": "<String>", "name": "<String>" }], "cc": { "address": "<String>", "name": "<String>" }, "cc_list": [{ "address": "<String>", "name": "<String>" }], "bcc": { "address": "<String>", "name": "<String>" }, "bcc_list": [{ "address": "<String>", "name": "<String>" }], }</pre>		
id	String	Поле заголовка Message-ID

Поле (объект)	Тип данных	Описание
references	String	Идентификационное поле заголовка references согласно RFC 5322
reply_to	String	Идентификационное поле заголовка in-reply-to согласно RFC 5322
subject	String	Тема письма
address	String	Адрес электронной почты
from_address	JSON object	Информация об отправителе письма
<Адресное поле> → address	String	Адрес электронной почты отправителя (получателя) письма
<Адресное поле> → name	String	Имя отправителя (получателя) письма
to	JSON object	Информация о получателе письма (первом из списка)
to_list	Array of JSON objects	Информация о получателях письма
cc	JSON object	Информация о получателе копии письма (первом из списка)
cc_list	Array of JSON objects	Информация о получателях копии письма
bcc	JSON object	Информация о получателе скрытой копии письма (первом из списка)
bcc_list	Array of JSON objects	Информация о получателях скрытой копии письма

Примеры

Пример сообщения при начале работы с источником:

```
<100>1 2024-01-15T07:22:44.018041Z example-host emailsecurity -
mail_gateway_mta.start - {
  "scan_id": "a36a1f7c-51af-32b1-a144-659b1dfe31c1",
  "created": 1511421763.3728465,
  "received": 1511421762.957363,
  "entry_point_id": "mail-gateway-mta",
  "client": {
    "ip": "203.0.113.33",
    "address": "203.0.113.33",
    "port": 36128
  },
  "envelope": {
    "from_address": "ivanov@example.org",
    "recipients": ["username@example.com"]
  },
  "email": {
    "id": "<6fee62f024e0@example.com>",
    "subject": "Последняя версия моей программы",
    "references": "",
    "reply_to": ""
    "from_address": {
      "address": "ivanov@example.org",
      "name": "Ivan Ivanov"
    },
    "to": {
      "address": "username@example.com",
      "name": "Ivan Ivanov"
    },
    "to_list": [
      {
        "address": "username@example.com",
        "name": "Ivan Ivanov"
      }
    ]
  }
}
```

3.3.8. Сообщение files_monitor.start

Сообщение отправляется при появлении файла в отслеживаемой общей папке.

Тело сообщения:

```
{
  "scan_id": "<String>",
  "created": <Float>,
  "received": <Float>,
  "entry_point_id": "<String>",
  "src_file_info": <JSON object>,
  "file": <JSON object>
}
```

Таблица 34. Поля сообщения files_monitor.start

Поле (объект)	Тип данных	Описание
scan_id	String	Идентификатор задания на проверку
created	Float	UNIX-время создания сообщения
received	Float	UNIX-время создания задания на проверку
entry_point_id	String	Название источника для проверки, указанное в веб-интерфейсе
src_file_info	JSON object	Информация о файле в общей папке
file	JSON object	Информация о файле
src_file_info		
<pre>{ "url": "<String>" }</pre>		
url	String	Путь к файлу в общей папке
file		
<pre>{ "md5": "<String>", "mime_type": "<String>", "name": "<String>", "sha1": "<String>", "sha256": "<String>", "size": <UInt64> }</pre>		
md5	String	Хеш-сумма файла, вычисленная по алгоритму MD5
mime_type	String	MIME-тип файла
name	String	Имя файла
sha1	String	Хеш-сумма файла, вычисленная по алгоритму SHA-1

Поле (объект)	Тип данных	Описание
sha256	String	Хеш-сумма файла, вычисленная по алгоритму SHA-256
size	UInt64	Размер файла в байтах

Примеры

Пример сообщения при начале работы с источником:

```
<100>1 2024-01-15T07:22:44.018041Z example-host emailsecurity - files_monitor.start -
{
  "scan_id": "a36a1f7c-51af-32b1-a144-659b1dfe31c1",
  "created": 1511421763.3728465,
  "received": 1511421762.957363,
  "entry_point_id": "shared-folder",
  "src_file_info": {
    "url": "smb://example.org/share/software.exe"
  },
  "file": {
    "mime_type": "application/x-dosexec; charset=binary",
    "md5": "11aced0fd6535f6e...1495ba1c7be00",
    "sha1": "45e50e2af429e44...6f59e46b18b60",
    "sha256": "23ef04408bb2c...7928e7caf3d7f",
    "size": 64000,
    "name": "software.exe"
  }
}
```

3.3.9. Сообщение files_inbox.start

Сообщение отправляется при добавлении объекта в папку-шлюз.

Тело сообщения:

```
{
  "scan_id": "<String>",
  "created": <Float>,
  "received": <Float>,
  "entry_point_id": "<String>",
  "src_file_info": <JSON object>,
  "file": <JSON object>
}
```

Таблица 35. Поля сообщения files_inbox.start

Поле (объект)	Тип данных	Описание
scan_id	String	Идентификатор задания на проверку
created	Float	UNIX-время создания сообщения
received	Float	UNIX-время создания задания на проверку
entry_point_id	String	Название источника для проверки, указанное в веб-интерфейсе
src_file_info	JSON object	Информация о файле в папке-шлюзе
file	JSON object	Информация о файле
src_file_info		
<pre>{ "url": "<String>" }</pre>		
url	String	Путь к файлу в папке-шлюзе
file		
<pre>{ "md5": "<String>", "mime_type": "<String>", "name": "<String>", "sha1": "<String>", "sha256": "<String>", "size": <UInt64> }</pre>		
md5	String	Хеш-сумма файла, вычисленная по алгоритму MD5
mime_type	String	MIME-тип файла
name	String	Имя файла
sha1	String	Хеш-сумма файла, вычисленная по алгоритму SHA-1
sha256	String	Хеш-сумма файла, вычисленная по алгоритму SHA-256
size	UInt64	Размер файла в байтах

Примеры

Пример сообщения при начале работы с источником:

```
<100>1 2024-01-15T07:22:44.018041Z example-host emailsecurity - files_inbox.start - {
  "scan_id": "a36a1f7c-51af-32b1-a144-659b1dfe31c1",
  "created": 1511421763.37285,
  "received": 1511421762.95736,
  "entry_point_id": "gateway-folder",
  "src_file_info": {
    "url": "smb://example.org/share/inbox/software.exe"
  },
  "file": {
    "md5": "11aced0fd6535f6e...1495ba1c7be00",
    "mime_type": "application/x-dosexec; charset=binary",
    "name": "software.exe",
    "sha1": "45e50e2af429e44...6f59e46b18b60",
    "sha256": "23ef04408bb2c...7928e7caf3d7f",
    "size": 64000
  }
}
```

3.3.10. Сообщение icap.start

Сообщение отправляется при получении объекта по ICAP.

Тело сообщения:

```
{
  "scan_id": "<String>",
  "created": <Float>,
  "received": <Float>,
  "entry_point_id": "<String>",
  "client": <JSON object>,
  "request": <JSON object>
}
```

Таблица 36. Поля сообщения icap.start

Поле (объект)	Тип данных	Описание
scan_id	String	Идентификатор задания на проверку
created	Float	UNIX-время создания сообщения
received	Float	UNIX-время создания задания на проверку
entry_point_id	String	Название источника для проверки, указанное в веб-интерфейсе

Поле (объект)	Тип данных	Описание
client	JSON object	Информация об ICAP-клиенте, который обращается к ICAP-серверу
request	JSON object	Информация о запросе
client		
<pre>{ "address": "<String>", "ip": "<String>", "port": <UInt32> }</pre>		
address	String	IP-адрес ICAP-клиента
ip	String	IP-адрес ICAP-клиента
port	UInt32	Порт ICAP-клиента
request		
<pre>{ "client_ip": "<String>", "client_username": "<String>", "method": "<String>", "url": "<String>", "version": "<String>", "file": <JSON object> или "http": <JSON object> }</pre>		
client_ip	String	IP-адрес пользователя, который получил контент или отправил HTTP-запрос. Значение извлекается из поля X-Client-IP заголовка HTTP-запроса
client_username	String	Имя пользователя, прошедшего аутентификацию на прокси-сервере. Значение извлекается из поля X-Client-Username заголовка HTTP-запроса
method	String	Метод запроса. Возможные значения: — REQMOD — запрос на изменение HTTP REQUEST; — RESPMOD — запрос на изменение HTTP RESPONSE
url	String	URL, по которому идет обращение по ICAP
version	String	Версия протокола ICAP-клиента
file	JSON object	Информация о файле

Поле (объект)	Тип данных	Описание
http	JSON object	Информация о файле из полей HTTP
request → file		
<pre>{ "md5": "<String>", "mime_type": "<String>", "name": "<String>", "sha1": "<String>", "sha256": "<String>", "size": "<UInt64>" }</pre>		
md5	String	Хеш-сумма файла, вычисленная по алгоритму MD5
mime_type	String	MIME-тип файла
name	String	Имя файла
sha1	String	Хеш-сумма файла, вычисленная по алгоритму SHA-1
sha256	String	Хеш-сумма файла, вычисленная по алгоритму SHA-256
size	UInt64	Размер файла в байтах
request → http		
<pre>{ "direction": "<Enum>", "http_request": <JSON object> или "http_response": <JSON object> }</pre>		
direction	Enum	Направление сообщения. Возможные значения: — REQUEST — запрос к удаленному узлу за прокси-сервером; — RESPONSE — ответ от удаленного узла за прокси-сервером
http_request	JSON object	Информация об HTTP-запросе. Записывается только в случае запроса к удаленному узлу за прокси-сервером, в остальных случаях поле отсутствует
http_response	JSON object	Информация об HTTP-ответе. Записывается только в случае ответа от удаленного узла за прокси-сервером, в остальных случаях поле отсутствует

Поле (объект)	Тип данных	Описание
request → http → http_request		
<pre>{ "content_disposition": { "filename": "<String>", "type": "<String>" }, "content_length": <UInt32>, "content_location": "<String>", "content_type": { "boundary": "<String>", "charset": "<String>", "mime_type": "<String>", "name": "<String>" }, "host": "<String>", "method": "<String>", "referer": "<String>", "url": "<String>", "user_agent": "<String>", "version": "<String>" }</pre>		
content_disposition	JSON object	Содержимое поля заголовка Content-Disposition
content_disposition → filename	String	Имя файла согласно полю Content-Disposition заголовка HTTP-сообщения
content_disposition → type	String	Тип файла согласно полю Content-Disposition заголовка HTTP-сообщения
content_length	UInt32	Содержимое поля заголовка Content-Length
content_location	String	Содержимое поля заголовка Content-Location
content_type	JSON object	Содержимое поля заголовка Content-Type
content_type → boundary	String	Значение параметра boundary в поле Content-Type заголовка HTTP-сообщения
content_type → charset	String	Кодировка веб-страницы
content_type → mime_type	String	MIME-тип файла согласно полю Content-Type заголовка HTTP-сообщения
content_type → name	String	Значение параметра name в поле Content-Type заголовка HTTP-сообщения

Поле (объект)	Тип данных	Описание
host	String	Доменное имя сервера, которому был адресован HTTP-запрос
method	String	Метод HTTP-запроса. Возможные значения: <code>get</code> или <code>post</code>
referer	String	Адрес предыдущей веб-страницы, с которой был осуществлен данный HTTP-запрос
url	String	URL HTTP-запроса
user_agent	String	Название пользовательского приложения (например, браузера), с которого был осуществлен HTTP-запрос
version	String	Версия HTTP

request → http → http_response

<pre>{ "code": <UInt32>, "content_disposition": { "filename": "<String>", "type": "<String>" }, "content_length": <UInt32>, "content_location": "<String>", "content_type": { "boundary": "<String>", "charset": "<String>", "mime_type": "<String>", "name": "<String>" }, "reason": "<String>", "server": "<String>", "version": "<String>" }</pre>		
code	UInt32	Код ответа
content_disposition	JSON object	Содержимое поля заголовка Content-Disposition
content_disposition → filename	String	Имя файла согласно полю Content-Disposition заголовка HTTP-сообщения
content_disposition → type	String	Тип файла согласно полю Content-Disposition заголовка HTTP-сообщения
content_length	UInt32	Содержимое поля заголовка Content-Length
content_location	String	Содержимое поля заголовка Content-Location

Поле (объект)	Тип данных	Описание
content_type	JSON object	Содержимое поля заголовка Content-Type
content_type → boundary	String	Значение параметра boundary в поле Content-Type заголовка HTTP-сообщения
content_type → charset	String	Кодировка веб-страницы
content_type → mime_type	String	MIME-тип файла согласно полю Content-Type заголовка HTTP-сообщения
content_type → name	String	Значение параметра name в поле Content-Type заголовка HTTP-сообщения
reason	String	Описание ответа (Reason-Phrase)
server	String	Название и версия веб-сервера, от которого был получен HTTP-ответ
version	String	Версия HTTP

Примеры

Пример сообщения при начале работы с источником:

```
<100>1 2024-01-15T07:22:44.018041Z example-host emailsecurity - icap.start - {
  "scan_id": "a36a1f7c-51af-32b1-a144-659b1dfe31c1",
  "created": 1511421763.37285,
  "received": 1511421762.95736,
  "entry_point_id": "icap",
  "client": {
    "address": "198.51.100.13",
    "ip": "198.51.100.13",
    "port": 55892
  },
  "request": {
    "client_ip": "198.51.100.22",
    "client_username": "",
    "method": "RESPMOD",
    "url": "icap://198.51.100.12:1344/bypass",
    "version": "1.0",
    "http": {
      "direction": "RESPONSE",
      "http_request": {
        "content_disposition": {
          "filename": "",
          "type": ""
        },
        "content_length": 0,
        "content_location": "",
        "content_type": {
          "boundary": "",
          "charset": "",
          "mime_type": "",
          "name": ""
        },
        "host": "203.0.113.152",
        "method": "GET",
        "referer": "http://203.0.113.152/MySample/",
        "url": "http://203.0.113.152/MySample/EICAR.COM",
        "user_agent": "Mozilla/5.0 (Windows NT 6.3; Win64; x64; rv:97.0) Gecko/20100101 Firefox/97.0",
        "version": "1.1"
      },
      "http_response": {
        "code": 200,
        "content_disposition": {
          "filename": "",
```

```

        "type": ""
    },
    "content_length": 9322,
    "content_location": "",
    "content_type": {
        "boundary": "",
        "charset": "",
        "mime_type": "application/octet-stream",
        "name": ""
    },
    "reason": "OK",
    "server": "nginx/1.16.1",
    "version": "1.1"
}
}
}
}

```

3.3.11. Сообщение dpi.start

Сообщение отправляется при получении объекта от PT NAD.

Тело сообщения:

```

{
  "scan_id": "<String>",
  "created": <Float>,
  "received": <Float>,
  "entry_point_id": "<String>",
  "file": <JSON object>,
  "meta": <JSON object>
}

```

Таблица 37. Поля сообщения dpi.start

Поле (объект)	Тип данных	Описание
scan_id	String	Идентификатор задания на проверку
created	Float	UNIX-время создания сообщения
received	Float	UNIX-время создания задания на проверку
entry_point_id	String	Название источника для проверки, указанное в веб-интерфейсе
file	JSON object	Информация о файле
meta	JSON object	Информация о запросе прикладного уровня, анализируемом с помощью технологии DPI

Поле (объект)	Тип данных	Описание
file		
<pre>{ "md5": "<String>", "mime_type": "<String>", "name": "<String>", "sha1": "<String>", "sha256": "<String>", "size": <UInt64> }</pre>		
md5	String	Хеш-сумма файла, вычисленная по алгоритму MD5
mime_type	String	MIME-тип файла
name	String	Имя файла
sha1	String	Хеш-сумма файла, вычисленная по алгоритму SHA-1
sha256	String	Хеш-сумма файла, вычисленная по алгоритму SHA-256
size	UInt64	Размер файла в байтах
meta		
<pre>{ "file_id": "<String>", "filename": "<String>", "magic": "<String>", "proto": "<String>", "state": "<Enum>", "http": <JSON object> или "smtp": <JSON object>, "src": <JSON object>, "dst": <JSON object> }</pre>		
file_id	String	Идентификатор полученного файла
filename	String	Имя файла
magic	String	Текстовое описание автоматически определенного формата файла
proto	String	Прикладной протокол, который использовался для передачи файла

Поле (объект)	Тип данных	Описание
state	String	Состояние записи файла: — COMPLETED — файл записан; — ERROR — ошибка записи (при получении ошибки файл удаляется); — TRUNCATED — файл записан не полностью, но данных больше нет; — UNKNOWN — состояние неизвестно. Проверяются только файлы с состоянием COMPLETED
http	JSON object	Информация о файле, относящаяся к HTTP
smtp	JSON object	Информация о файле, относящаяся к SMTP
src	JSON object	Информация об отправителе файла
dst	JSON object	Информация о получателе файла

meta → http

<pre>{ "host": "<String>", "referer": "<String>", "uri": "<String>", "user_agent": "<String>" }</pre>		
host	String	HTTP-адрес узла, с которого был скачан файл
referer	String	Адрес предыдущей веб-страницы, с которой был выполнен переход
uri	String	URI файла
user_agent	String	Название и версия браузера

meta → smtp

<pre>{ "message_id": "<String>", "sender": "<String>" }</pre>		
message_id	String	Поле заголовка Message-ID
sender	String	Адрес электронной почты отправителя

Поле (объект)	Тип данных	Описание
meta → src		
<pre>{ "address": "<String>", "ip": "<String>", "port": <UInt32> }</pre>		
address	String	IP-адрес
ip	String	IP-адрес
port	UInt32	Номер сетевого порта
meta → dst		
<pre>{ "address": "<String>", "ip": "<String>", "port": <UInt32> }</pre>		
address	String	IP-адрес
ip	String	IP-адрес
port	UInt32	Номер сетевого порта

Примеры

Пример сообщения при начале работы с источником:

```
<100>1 2024-01-15T07:22:44.018041Z example-host emailsecurity - dpi.start - {
  "scan_id": "a36a1f7c-51af-32b1-a144-659b1dfe31c1",
  "created": 1511421763.37285,
  "entry_point_id": "dpi-module",
  "received": 1511421762.95736,
  "file": {
    "md5": "11aced0fd6535f6e...1495ba1c7be00",
    "mime_type": "application/x-dosexec; charset=binary",
    "name": "software.exe",
    "sha1": "45e50e2af429e44...6f59e46b18b60",
    "sha256": "23ef04408bb2c...7928e7caf3d7f",
    "size": 64000
  },
  "meta": {
    "dst": {
      "address": "203.0.113.11",
      "ip": "203.0.113.11",
      "port": 8080
    },
    "file_id": "10007",
    "filename": "example",
    "http": {
      "host": "203.0.113.43",
      "referer": "<unknown>",
      "uri": "/test",
      "user_agent": "Wget/1.15 (linux-gnu)"
    },
    "magic": "ASCII text, with very long lines",
    "proto": "HTTP",
    "src": {
      "address": "203.0.113.43",
      "ip": "203.0.113.43",
      "port": 8080
    },
    "state": "COMPLETED"
  }
}
```

3.3.12. Сообщение retro.start

Сообщение отправляется при запуске повторной проверки файлов в хранилище.

Тело сообщения:

```
{
  "scan_id": "<String>",
  "created": <Float>,
  "received": <Float>
}
```

Таблица 38. Поля сообщения retro.start

Поле (объект)	Тип данных	Описание
scan_id	String	Идентификатор задания на проверку
created	Float	UNIX-время создания сообщения
received	Float	UNIX-время создания задания на проверку

Примеры

Пример сообщения при начале работы с источником:

```
<100>1 2024-01-15T07:22:44.018041Z example-host emailsecurity - retro.start - {
  "scan_id": "a36a1f7c-51af-32b1-a144-659b1dfe31c1",
  "created": 1511421763.37285,
  "received": 1511421762.95736
}
```

3.3.13. Сообщение public_api.start

Сообщение отправляется при получении объекта от сервиса публичного API при проверке с передаваемыми параметрами.

Тело сообщения:

```
{
  "scan_id": "<String>",
  "created": <Float>,
  "received": <Float>,
  "entry_point_id": "<String>",
  "origin_ip": "<String>",
  "peer_ip": "<String>",
  "file": <JSON object>,
  "http_headers": <JSON object>
}
```

Таблица 39. Поля сообщения public_api.start

Поле (объект)	Тип данных	Описание
scan_id	String	Идентификатор задания на проверку

Поле (объект)	Тип данных	Описание
created	Float	UNIX-время создания сообщения
received	Float	UNIX-время создания задания на проверку
entry_point_id	String	Название источника для проверки, указанное в веб-интерфейсе
origin_ip	String	Первый IP-адрес из цепочки адресов, записанных в HTTP-заголовке X-Forwarded-For
peer_ip	String	Фактический IP-адрес приложения, отправившего файл на проверку
file	JSON object	Информация о файле
http_headers	JSON object	Информация об HTTP-заголовках в запросе приложения, отправившего файл на проверку

file

```
{
  "md5": "<String>",
  "mime_type": "<String>",
  "name": "<String>",
  "sha1": "<String>",
  "sha256": "<String>",
  "size": <UInt64>
}
```

md5	String	Хеш-сумма файла, вычисленная по алгоритму MD5
mime_type	String	MIME-тип файла
name	String	Имя файла
sha1	String	Хеш-сумма файла, вычисленная по алгоритму SHA-1
sha256	String	Хеш-сумма файла, вычисленная по алгоритму SHA-256
size	UInt64	Размер файла в байтах

http_headers

```
{
  "referer": "<String>",
  "user_agent": "<String>",
  "x_forwarded_for": "<String>"
}
```

referer	String	Значение в HTTP-заголовке Referer
user_agent	String	Значение в HTTP-заголовке User-Agent

Поле (объект)	Тип данных	Описание
x_forwarded_for	String	Значение в HTTP-заголовке X-Forwarded-For

Примеры

Пример сообщения при начале работы с источником:

```
<100>1 2024-01-15T07:22:44.018041Z example-host emailsecurity - public_api.start - {
  "scan_id": "a36a1f7c-51af-32b1-a144-659b1dfe31c1",
  "created": 1511421763.3728465,
  "received": 1511421762.957363,
  "entry_point_id": "api-service",
  "origin_ip": "198.51.100.1",
  "peer_ip": "198.51.100.1",
  "file": {
    "md5": "11aced0fd6535f6e...1495ba1c7be00",
    "mime_type": "",
    "name": "software.exe"
    "sha1": "45e50e2af429e44...6f59e46b18b60",
    "sha256": "23ef04408bb2c...7928e7caf3d7f",
    "size": 64000
  },
  "http_headers": {
    "user_agent": "curl/7.68.0",
    "x_forwarded_for": "198.51.100.1",
    "referer": ""
  }
}
```

3.3.14. Сообщение scan_api.start

Сообщение отправляется при получении объекта от сервиса публичного API при проверке с параметрами источника.

Тело сообщения:

```
{
  "scan_id": "<String>",
  "created": <Float>,
  "received": <Float>,
  "entry_point_id": "<String>",
  "origin_ip": "<String>",
  "peer_ip": "<String>",
  "file": <JSON object>,
  "http_headers": <JSON object>
}
```

Таблица 40. Поля сообщения scan_api.start

Поле (объект)	Тип данных	Описание
scan_id	String	Идентификатор задания на проверку
created	Float	UNIX-время создания сообщения
received	Float	UNIX-время создания задания на проверку
entry_point_id	String	Название источника для проверки, указанное в веб-интерфейсе
origin_ip	String	Первый IP-адрес из цепочки адресов, записанных в HTTP-заголовке X-Forwarded-For
peer_ip	String	Фактический IP-адрес приложения, отправившего файл на проверку
file	JSON object	Информация о файле
http_headers	JSON object	Информация об HTTP-заголовках в запросе приложения, отправившего файл на проверку

file

```
{
  "md5": "<String>",
  "mime_type": "<String>",
  "name": "<String>",
  "sha1": "<String>",
  "sha256": "<String>",
  "size": <UInt64>
}
```

md5	String	Хеш-сумма файла, вычисленная по алгоритму MD5
mime_type	String	MIME-тип файла
name	String	Имя файла
sha1	String	Хеш-сумма файла, вычисленная по алгоритму SHA-1
sha256	String	Хеш-сумма файла, вычисленная по алгоритму SHA-256
size	UInt64	Размер файла в байтах

http_headers

```
{
  "referer": "<String>",
  "user_agent": "<String>",
  "x_forwarded_for": "<String>"
}
```

Поле (объект)	Тип данных	Описание
referer	String	Значение в HTTP-заголовке Referer
user_agent	String	Значение в HTTP-заголовке User-Agent
x_forwarded_for	String	Значение в HTTP-заголовке X-Forwarded-For

Примеры

Пример сообщения при начале работы с источником:

```
<100>1 2024-01-15T07:22:44.018041Z example-host emailsecurity - scan_api.start - {
  "scan_id": "a36a1f7c-51af-32b1-a144-659b1dfe31c1",
  "created": 1511421763.3728465,
  "received": 1511421762.957363,
  "entry_point_id": "api-service",
  "origin_ip": "198.51.100.1",
  "peer_ip": "198.51.100.1",
  "file": {
    "md5": "11aced0fd6535f6e...1495ba1c7be00",
    "mime_type": "",
    "name": "software.exe"
    "sha1": "45e50e2af429e44...6f59e46b18b60",
    "sha256": "23ef04408bb2c...7928e7caf3d7f",
    "size": 64000
  },
  "http_headers": {
    "user_agent": "curl/7.68.0",
    "x_forwarded_for": "198.51.100.1",
    "referer": ""
  }
}
```

3.3.15. Сообщение pt_edr.start

Сообщение отправляется при получении файлов конечных устройств от источника MaxPatrol EDR.

Тело сообщения:

```
{
  "scan_id": "<String>",
  "created": <Float>,
  "received": <Float>,
  "entry_point_id": "<String>",
  "origin_ip": "<String>",
  "peer_ip": "<String>",
  "file": <JSON object>,
  "http_headers": <JSON object>
}
```

Таблица 41. Поля сообщения pt_edr.start

Поле (объект)	Тип данных	Описание
scan_id	String	Идентификатор задания на проверку
created	Float	UNIX-время создания сообщения
received	Float	UNIX-время создания задания на проверку
entry_point_id	String	Название источника для проверки, указанное в веб-интерфейсе
origin_ip	String	Первый IP-адрес из цепочки адресов, записанных в HTTP-заголовке X-Forwarded-For
peer_ip	String	Фактический IP-адрес приложения, отправившего файл на проверку
file	JSON object	Информация о файле
http_headers	JSON object	Информация об HTTP-заголовках в запросе приложения, отправившего файл на проверку
file		
<pre>{ "md5": "<String>", "mime_type": "<String>", "name": "<String>", "sha1": "<String>", "sha256": "<String>", "size": <UInt64> }</pre>		
md5	String	Хеш-сумма файла, вычисленная по алгоритму MD5
mime_type	String	MIME-тип файла
name	String	Имя файла

Поле (объект)	Тип данных	Описание
sha1	String	Хеш-сумма файла, вычисленная по алгоритму SHA-1
sha256	String	Хеш-сумма файла, вычисленная по алгоритму SHA-256
size	UInt64	Размер файла в байтах

http_headers

<pre>{ "user_agent": "<String>", "x_forwarded_for": "<String>" "referer": "<String>", "x_source_metadata": "<JSON object>" }</pre>		
user_agent	String	Значение HTTP-заголовка User-Agent
x_forwarded_for	String	Значение HTTP-заголовка X-Forwarded-For
referer	String	Значение HTTP-заголовка Referer
x_source_metadata	JSON object	Значения HTTP-заголовка метаданных источника. Ключ и значение типа String

Примеры

Пример сообщения при начале работы с источником:

```
<100>1 2024-01-15T07:22:44.018041Z example-host emailsecurity - pt_edr.start - {
  "scan_id": "a36a1f7c-51af-32b1-a144-659b1dfe31c1",
  "created": 1511421763.3728465,
  "entry_point_id": "pt-edr",
  "received": 1511421762.957363,
  "http_headers": {
    "user_agent": "curl/7.68.0",
    "x_forwarded_for": "198.51.100.1",
    "referer": ""
  },
  "x_source_metadata": {
    "Asset.Host.IpAddress": "198.51.100.1",
    "User.OsUser": "root"
  }
},
"origin_ip": "198.51.100.1",
"peer_ip": "198.51.100.1",
"file": {
  "sha256": "23ef04408bb2c...7928e7caf3d7f",
  "md5": "11aced0fd6535f6e...1495ba1c7be00",
  "sha1": "45e50e2af429e44...6f59e46b18b60",
  "mime_type": "",
  "size": 64000,
  "name": "software.exe"
}
}
```

3.4. Добавление объекта, new_artifact

Сообщение отправляется при появлении нового объекта. Это может быть исходный объект задания, поступивший на проверку от источника, или дочерний объект, полученный в ходе выполнения задания или проверки. Для дочерних объектов в сообщении указывается информация о родительском объекте, это позволяет составить иерархию объектов задания.

Тело сообщения:

```
{
  "scan_id": "<String>",
  "created": <Float>,
  "entry_point_id": "<String>",
  "entry_point_type": "<Enum>",
  "parent": <JSON object>,
  "new_artifact": <JSON object>
}
```

Таблица 42. Поля сообщения new_artifact

Поле (объект)	Тип данных	Описание
scan_id	String	Идентификатор задания на проверку
created	Float	UNIX-время создания сообщения
entry_point_id	String	Название источника для проверки, указанное в веб-интерфейсе
entry_point_type	Enum	Тип источника (см. раздел 3.9)
parent	JSON object	Информация о родительском объекте: — file — файл-контейнер, из которого извлечен объект, или файл процесса, запуск которого привел к созданию объекта; — url — ссылка, по которой скачан объект
new_artifact	JSON object	Информация об объекте. Содержит один из JSON-объектов: — file — файл; — url — ссылка; — sandbox_amsi — AMSI-скрипт; — sandbox_drop — dropped файл; — sandbox_process_memory_dump — дамп памяти (procdump); — sandbox_memory_dump — дамп памяти (memdump)

parent		
<pre>{ "file": <JSON object> или "url": <JSON object> }</pre>		
file	JSON object	Информация о файле
url	JSON object	Информация о ссылке

Поле (объект)	Тип данных	Описание
parent → file		
<pre>{ "md5": "<String>", "mime_type": "<String>", "name": "<String>", "sha1": "<String>", "sha256": "<String>", "size": <UInt64> }</pre>		
md5	String	Хеш-сумма файла, вычисленная по алгоритму MD5
mime_type	String	MIME-тип файла
name	String	Имя файла
sha1	String	Хеш-сумма файла, вычисленная по алгоритму SHA-1
sha256	String	Хеш-сумма файла, вычисленная по алгоритму SHA-256
size	UInt64	Размер файла в байтах
parent → url		
<pre>{ "value": "<String>" }</pre>		
value	String	Ссылка
new_artifact		
<pre>{ "file": <JSON object>, "url": <JSON object>, "sandbox_drop": <JSON object>, "sandbox_process_memory_dump": <JSON object> или "sandbox_memory_dump": <JSON object> }</pre>		
file	JSON object	Информация о файле
url	JSON object	Информация о ссылке
sandbox_drop	JSON object	Информация о файле, который создал, удалил или с которым взаимодействовал проверяемый файл в ходе поведенческого анализа
sandbox_process_memory_dump	JSON object	Информация о дампе памяти, относящемся к процессу, за которым велось наблюдение в ходе поведенческого анализа. Дамп созда-

Поле (объект)	Тип данных	Описание
		ется после штатного завершения процесса или по истечении времени наблюдения за файлом
sandbox_memory_dump	JSON object	Информация о дампе памяти, относящемся к процессу, за которым велось наблюдение в ходе поведенческого анализа. Дамп создается при наступлении события, значимого для поведенческого анализа

new_artifact → file

<pre>{ "md5": "<String>", "mime_type": "<String>", "name": "<String>", "sha1": "<String>", "sha256": "<String>", "size": <UInt64> }</pre>		
md5	String	Хеш-сумма файла, вычисленная по алгоритму MD5
mime_type	String	MIME-тип файла
name	String	Имя файла
sha1	String	Хеш-сумма файла, вычисленная по алгоритму SHA-1
sha256	String	Хеш-сумма файла, вычисленная по алгоритму SHA-256
size	UInt64	Размер файла в байтах

new_artifact → url

<pre>{ "value": "<String>" }</pre>		
value	String	Ссылка

Поле (объект)	Тип данных	Описание
new_artifact → sandbox_drop		
<pre>{ "dump_create_time": <Float>, "dump_trigger": "<String>", "md5": "<String>", "mime_type": "<String>", "name": "<String>", "process_id": <UInt32>, "process_name": "<String>", "sha1": "<String>", "sha256": "<String>", "size": <UInt64> }</pre>		
dump_create_time	Float	UNIX-время создания артефакта
dump_trigger	String	Название события, которое спровоцировало создание дампа памяти (например, TerminateProcess или Possible shellcode detected)
md5	String	Хеш-сумма файла, вычисленная по алгоритму MD5
mime_type	String	MIME-тип файла
name	String	Имя файла
process_id	UInt32	Идентификатор процесса, по которому был создан артефакт
process_name	String	Название процесса, по которому был создан артефакт
sha1	String	Хеш-сумма файла, вычисленная по алгоритму SHA-1
sha256	String	Хеш-сумма файла, вычисленная по алгоритму SHA-256
size	UInt64	Размер файла в байтах

Поле (объект)	Тип данных	Описание
new_artifact → sandbox_process_memory_dump		
<pre>{ "dump_create_time": <Float>, "dump_trigger": "<String>", "md5": "<String>", "mime_type": "<String>", "name": "<String>", "process_id": <UInt32>, "process_name": "<String>", "sha1": "<String>", "sha256": "<String>", "size": <UInt64> }</pre>		
dump_create_time	Float	UNIX-время создания артефакта
dump_trigger	String	Название события, которое спровоцировало создание дампа памяти (например, TerminateProcess или Possible shellcode detected)
md5	String	Хеш-сумма файла, вычисленная по алгоритму MD5
mime_type	String	MIME-тип файла
name	String	Имя файла
process_id	UInt32	Идентификатор процесса, по которому был создан артефакт
process_name	String	Название процесса, по которому был создан артефакт
sha1	String	Хеш-сумма файла, вычисленная по алгоритму SHA-1
sha256	String	Хеш-сумма файла, вычисленная по алгоритму SHA-256
size	UInt64	Размер файла в байтах

Поле (объект)	Тип данных	Описание
new_artifact → sandbox_memory_dump		
<pre>{ "dump_create_time": <Float>, "dump_trigger": "<String>", "md5": "<String>", "mime_type": "<String>", "name": "<String>", "process_id": <UInt32>, "process_name": "<String>", "sha1": "<String>", "sha256": "<String>", "size": <UInt64> }</pre>		
dump_create_time	Float	UNIX-время создания артефакта
dump_trigger	String	Название события, которое спровоцировало создание дампа памяти (например, TerminateProcess или Possible shellcode detected)
md5	String	Хеш-сумма файла, вычисленная по алгоритму MD5
mime_type	String	MIME-тип файла
name	String	Имя файла
process_id	UInt32	Идентификатор процесса, по которому был создан артефакт
process_name	String	Название процесса, по которому был создан артефакт
sha1	String	Хеш-сумма файла, вычисленная по алгоритму SHA-1
sha256	String	Хеш-сумма файла, вычисленная по алгоритму SHA-256
size	UInt64	Размер файла в байтах

Примеры

Пример сообщения для файла:

```
<100>1 2024-01-15T07:22:44.018041Z example-host emailsecurity - new_artifact - {
  "scan_id": "a36a1f7c-51af-32b1-a144-659b1dfe31c1",
  "created": 1511421763.3728465,
  "entry_point_id": "example_source_name",
  "entry_point_type": "icap",
  "new_artifact": {
    "file": {
      "mime_type": "",
      "md5": "11aced0fd6535f6e...1495ba1c7be00",
      "sha1": "45e50e2af429e44...6f59e46b18b60",
      "sha256": "23ef04408bb2c...7928e7caf3d7f",
      "size": 64000,
      "name": "software.exe"
    }
  }
}
```

Пример сообщения для ссылки:

```
<100>1 2024-01-15T07:22:44.018041Z example-host emailsecurity - new_artifact - {
  "scan_id": "d2157391-6fd6-11ed-8002-cfcd208495d5",
  "created": 1669720395.66726,
  "entry_point_id": "example_source_name",
  "entry_point_type": "icap",
  "new_artifact": {
    "url": {
      "value": "http://example.com"
    }
  }
}
```

Пример сообщения для dropped файла:

```
<100>1 2024-01-15T07:22:44.018041Z example-host emailsecurity - new_artifact - {
  "scan_id": "a36a1f7c-51af-32b1-a144-659b1dfe31c1",
  "created": 1511421763.3728465,
  "entry_point_id": "example_source_name",
  "entry_point_type": "icap",
  "parent": {
    "file": {
      "sha256": "23ef04408bb2c...7928e7caf3d7f",
      "mime_type": "text/x-msdos-batch",
      "md5": "11aced0fd6535f6e...1495ba1c7be00",
      "sha1": "45e50e2af429e44...6f59e46b18b60",
      "name": "sc.exe",
      "size": 64000
    }
  },
  "new_artifact": {
    "sandbox_drop": {
      "mime_type": "",
      "md5": "11aced0fd6535f6e...1495ba1c7be00",
      "sha1": "45e50e2af429e44...6f59e46b18b60",
      "sha256": "23ef04408bb2c...7928e7caf3d7f",
      "size": 40,
      "process_name": "windows/system32/sppsvc.exe",
      "process_id": 4568,
      "dump_trigger": "",
      "dump_create_time": 30.801,
      "name": "users/john/appdata/local/google/chrome/user data/crashpad/
settings.dat"
    }
  }
}
```

3.5. Проверка объекта

При проверке объекта PT Email Security отправляет сообщения с результатами проверки, указанные в таблице. В разделе описаны форматы этих сообщений.

Таблица 43. Типы сообщений, отправляемых в ходе проверки объектов

Тип сообщения	Когда регистрируется
scan_machine.new_object	В ходе проверки обнаружен новый объект
scan_machine.file_result.av	Объект проверен одним из средств проверки (см. раздел 3.10)

Тип сообщения	Когда регистрируется
<code>scan_machine.file_result.pt_sandbox</code>	Объект проверен методом поведенческого анализа
<code>scan_machine.file_result.meldd</code>	Вынесен вердикт по объекту на основании результатов проверок объекта всеми средствами проверки и вердиктов дочерних объектов
<code>scan_machine.final_result</code>	Вынесен вердикт по заданию на основании вердикта исходного объекта задания и вердиктов дочерних объектов

В этом разделе

[Сообщение `scan\_machine.new\_object` \(см. раздел 3.5.1\)](#)

[Сообщение `scan\_machine.file\_result.av` \(см. раздел 3.5.2\)](#)

[Сообщение `scan\_machine.file\_result.pt\_sandbox` \(см. раздел 3.5.3\)](#)

[Сообщение `scan\_machine.file\_result.meldd` \(см. раздел 3.5.4\)](#)

[Сообщение `scan\_machine.final\_result` \(см. раздел 3.5.5\)](#)

3.5.1. Сообщение `scan_machine.new_object`

Сообщение отправляется при появлении дочернего объекта в ходе проверки.

Тело сообщения:

```
{
  "scan_id": "<String>",
  "created": <Float>,
  "entry_point_id": "<String>",
  "entry_point_type": "<Enum>",
  "origin_file": <JSON object>,
  "recognized_object": <JSON object>
}
```

Таблица 44. Поля сообщения `scan_machine.new_object`

Поле (объект)	Тип данных	Описание
<code>scan_id</code>	String	Идентификатор задания на проверку
<code>created</code>	Float	UNIX-время создания сообщения
<code>entry_point_id</code>	String	Название источника для проверки, указанное в веб-интерфейсе
<code>entry_point_type</code>	Enum	Тип источника (см. раздел 3.9)

Поле (объект)	Тип данных	Описание
origin_file	JSON object	Информация о родительском объекте
recognized_object	JSON object	Информация о дочернем объекте: — archive — архив; — compressed_file — сжатый файл; — email — письмо; — file — файл
origin_file		
<pre>{ "md5": "<String>", "mime_type": "<String>", "name": "<String>", "sha1": "<String>", "sha256": "<String>", "size": <UInt64> }</pre>		
md5	String	Хеш-сумма файла, вычисленная по алгоритму MD5
mime_type	String	MIME-тип файла
name	String	Имя файла
sha1	String	Хеш-сумма файла, вычисленная по алгоритму SHA-1
sha256	String	Хеш-сумма файла, вычисленная по алгоритму SHA-256
size	UInt64	Размер файла в байтах
recognized_object		
<pre>{ "archive": <JSON object>, "compressed_file": <JSON object>, "email": <JSON object> или "file": <JSON object> }</pre>		
archive	JSON object	Информация об архиве
compressed_file	JSON object	Информация о сжатом файле
email	JSON object	Информация об электронном письме

Поле (объект)	Тип данных	Описание
file	JSON object	Информация о файле
recognized_object → archive		
<pre>{ "mime_type": "<String>" }</pre>		
mime_type	String	MIME-тип архива
recognized_object → compressed_file		
<pre>{ "file": { "md5": "<String>", "mime_type": "<String>", "name": "<String>", "sha1": "<String>", "sha256": "<String>", "size": <UInt64> }, "mime_type": "<String>" }</pre>		
file	JSON object	Информация о файле
file → md5	String	Хеш-сумма файла, вычисленная по алгоритму MD5
file → mime_type	String	MIME-тип файла
file → name	String	Имя файла
file → sha1	String	Хеш-сумма файла, вычисленная по алгоритму SHA-1
file → sha256	String	Хеш-сумма файла, вычисленная по алгоритму SHA-256
file → size	UInt64	Размер файла в байтах
mime_type	String	MIME-тип сжатого файла

Поле (объект)	Тип данных	Описание
recognized_object → email		
<pre>{ "id": "<String>", "references": "<String>", "reply_to": "<String>", "subject": "<String>", "from_address": { "address": "<String>", "name": "<String>" }, "bcc": { "address": "<String>", "name": "<String>" }, "bcc_list": [{ "address": "<String>", "name": "<String>" }], "cc": { "address": "<String>", "name": "<String>" }, "cc_list": [{ "address": "<String>", "name": "<String>" }], "to": { "address": "<String>", "name": "<String>" }, "to_list": [{ "address": "<String>", "name": "<String>" }] }</pre>		
id	String	Поле заголовка Message-ID

Поле (объект)	Тип данных	Описание
references	String	Идентификационное поле заголовка references согласно RFC 5322
reply_to	String	Идентификационное поле заголовка in-reply-to согласно RFC 5322
subject	String	Тема письма
address	String	Адрес электронной почты
from_address	JSON object	Информация об отправителе письма
<Адресное поле> → address	String	Адрес электронной почты отправителя (получателя) письма
<Адресное поле> → name	String	Имя отправителя (получателя) письма
to	JSON object	Информация о получателе письма (первом из списка)
to_list	Array of JSON objects	Информация о получателях письма
cc	JSON object	Информация о получателе копии письма (первом из списка)
cc_list	Array of JSON objects	Информация о получателях копии письма
bcc	JSON object	Информация о получателе скрытой копии письма (первом из списка)
bcc_list	Array of JSON objects	Информация о получателях скрытой копии письма
recognized_object → file		
<pre>{ "md5": "<String>", "mime_type": "<String>", "name": "<String>", "sha1": "<String>", "sha256": "<String>", "size": <UInt64> }</pre>		
md5	String	Хеш-сумма файла, вычисленная по алгоритму MD5

Поле (объект)	Тип данных	Описание
mime_type	String	MIME-тип файла
name	String	Имя файла
sha1	String	Хеш-сумма файла, вычисленная по алгоритму SHA-1
sha256	String	Хеш-сумма файла, вычисленная по алгоритму SHA-256
size	UInt64	Размер файла в байтах

Примеры

Пример сообщения при извлечении файла из архива:

```
<100>1 2024-01-15T07:22:44.018041Z example-host emailsecurity -
scan_machine.new_object - {
  "scan_id": "a36a1f7c-51af-32b1-a144-659b1dfe31c1",
  "created": 1511421763.3728465,
  "entry_point_id": "example_source_name",
  "entry_point_type": "icap",
  "origin_file": {
    "mime_type": "",
    "md5": "b53173def106ad...0ea30e504ec860f",
    "sha1": "c73c71d7858b7...de0272ce1125e01",
    "sha256": "d523708fe3b...e8f9a41b25f3c8d",
    "size": 792
  },
  "recognized_object": {
    "archive": {
      "mime_type": "application/zip; charset=binary"
    }
  }
}
```

3.5.2. Сообщение scan_machine.file_result.av

Сообщение отправляется при завершении проверки объекта одним из средств проверки.

Тело сообщения:

```
{
  "scan_id": "<String>",
  "created": <Float>,
  "av_code_name": "<String>",
  "database_time": <Float>,
  "duration": <Float>,
  "engine_version": "<String>",
  "entry_point_id": "<String>",
  "entry_point_type": "<Enum>",
  "file": <JSON-object> или "url": <JSON-object>
  "result": <JSON-object>
}
```

Таблица 45. Поля сообщения scan_machine.file_result.av

Поле (объект)	Тип данных	Описание
scan_id	String	Идентификатор задания на проверку
created	Float	UNIX-время создания сообщения
av_code_name	String	Название средства проверки, которым проверен объект (см. раздел 3.10)
database_time	Float	UNIX-время последнего обновления базы средства проверки
duration	Float	Продолжительность проверки в секундах
engine_version	String	Версия средства проверки
entry_point_id	String	Название источника для проверки, указанное в веб-интерфейсе
entry_point_type	Enum	Тип источника (см. раздел 3.9)
file	JSON-object	Информация о проверяемом файле
url	JSON-object	Информация о проверяемой ссылке
result	JSON object	Результат проверки, ошибки и состояние сканирования

Поле (объект)	Тип данных	Описание
file		
<pre>{ "md5": "<String>", "mime_type": "<String>", "name": "<String>", "sha1": "<String>", "sha256": "<String>", "size": <UInt64> }</pre>		
md5	String	Хеш-сумма файла, вычисленная по алгоритму MD5
mime_type	String	MIME-тип файла
name	String	Имя файла
sha1	String	Хеш-сумма файла, вычисленная по алгоритму SHA-1
sha256	String	Хеш-сумма файла, вычисленная по алгоритму SHA-256
size	UInt64	Размер файла в байтах
url		
<pre>{ "value": "<String>" }</pre>		
value	String	Ссылка
result		
<pre>{ "errors": <JSON object>, "raw_detections": <Array of strings>, "state": "<Enum>", "verdict": <JSON object> }</pre>		
errors	JSON object	Ошибки проверки
raw_detections	Array of strings	Результат проверки средством проверки в исходном виде. Например, для антивируса будет указано название обнаруженного вредоносного ПО, для средства проверки PT IoC будет указан тип обнаруженного индикатора компрометации: <i>byDomain</i> — домен, <i>byIp</i> — IP-адрес или <i>byUrl</i> — ссылка

Поле (объект)	Тип данных	Описание
state	String	Статус проверки объекта: — UNSCANNED — не проверен из-за ошибки; — PARTIAL — проверен частично; — FULL — проверен
verdict	JSON object	Информация о результате проверки

result → errors

<pre>{ "corrupted": <Boolean>, "encrypted": <Boolean>, "internal": <Boolean>, "limit_exceeded": <Boolean> }</pre>		
corrupted	Boolean	Файл поврежден
encrypted	Boolean	Файл зашифрован паролем, который неизвестен продукту
internal	Boolean	Внутренняя ошибка при проверке
limit_exceeded	Boolean	Проверка файла остановлена по лимиту (например, превышен максимально допустимый уровень вложенности архивов или максимальный размер файла)

result → verdict

<pre>{ "accuracy": <Float>, "threat": { "classification": "<Enum>", "family": "<String>", "platform": "<Enum>" }, "threat_level": "<Enum>" }</pre>		
accuracy	Float	Точность результата проверки
threat	JSON object	Информация об обнаруженной угрозе
threat → classification	Enum	Тип обнаруженного вредоносного ПО (см. раздел 3.11)
threat → family	String	Семейство, к которому принадлежит обнаруженное вредоносное ПО

Поле (объект)	Тип данных	Описание
threat → platform	Enum	Семейство операционных систем, на которое нацелено вредоносное ПО: — ANDROID; — IOS; — LINUX; — OSX; — WINDOWS; — NO_PLATFORM — семейство операционных систем не было определено
threat_level	Enum	Результат проверки объекта: — CLEAN — без обнаруженных угроз; — DANGEROUS — опасный; — UNKNOWN — результат неизвестен; — UNWANTED — потенциально опасный

Примеры

Пример сообщения с результатом проверки файла антивирусом ClamAV:

```
<100>1 2024-01-15T07:22:44.018041Z example-host emailsecurity -
scan_machine.file_result.av - {
  "scan_id": "a36a1f7c-51af-32b1-a144-659b1dfe31c1",
  "created": 1511421763.3728465,
  "av_code_name": "clamav",
  "database_time": 1510892498.0,
  "duration": 0.1300000,
  "engine_version": "0.99.2",
  "entry_point_id": "example_source_name",
  "entry_point_type": "icap",
  "file": {
    "mime_type": "application/x-dosexec; charset=binary",
    "md5": "11aced0fd6535f6e...1495ba1c7be00",
    "name": "software.exe",
    "sha1": "45e50e2af429e44...6f59e46b18b60",
    "sha256": "d523708fe3b...e8f9a41b25f3c8d",
    "size": 64000
  },
  "result": {
    "errors": {
      "internal": false,
      "corrupted": false,
      "encrypted": false
    },
    "raw_detections": [],
    "state": "FULL",
    "verdict": {
      "threat_level": "CLEAN",
      "threat": {
        "classification": "UNKNOWN",
        "platform": "NO_PLATFORM",
        "family": ""
      },
      "accuracy": 1.0
    }
  }
}
```

Пример сообщения с результатом проверки ссылки средством обнаружения индикаторов компрометации PT IoC:

```
<100>1 2024-01-15T07:22:44.018041Z example-host emailsecurity -
scan_machine.file_result.av - {
  "scan_id": "7e118bcf-b067-11ee-8192-3e4c81b2c1eb",
  "created": 1704966903.86009,
  "av_code_name": "ptioc",
  "database_time": 1704886178.0,
  "duration": 0.0,
  "engine_version": "5.8.0.65390",
  "entry_point_id": "example_source_name",
  "entry_point_type": "icap",
  "url": {
    "value": "https://example.org/site.com"
  },
  "result": {
    "errors": {
      "corrupted": false,
      "encrypted": false,
      "internal": false,
      "limit_exceeded": false
    },
    "raw_detections": [
      "byUrl"
    ],
    "state": "FULL",
    "verdict": {
      "threat": {
        "classification": "TROJAN",
        "family": "Unknown",
        "platform": "NO_PLATFORM"
      },
      "threat_level": "DANGEROUS"
    }
  }
}
```

3.5.3. Сообщение scan_machine.file_result.pt_sandbox

Сообщение отправляется при завершении поведенческого анализа файла.

Тело сообщения:

```
{
  "scan_id": "<String>",
  "created": <Float>,
  "analysis_duration": <Float>,
  "analysis_planned_duration": <Float>,
  "correlation_rules_version": "<String>",
  "detects": <Array of strings>,
  "dpi_rules_version": "<String>",
  "entry_point_id": "<String>",
  "entry_point_type": "<Enum>",
  "is_from_cache": <Boolean>,
  "source_created": <Float>,
  "source_scan_id": "<String>",
  "file": <JSON object>,
  "image_info": <JSON object>,
  "suspicious_behaviors": <Array of JSON objects>,
  "result": <JSON object>
}
```

Таблица 46. Поля сообщения scan_machine.file_result.pt_sandbox

Поле (объект)	Тип данных	Описание
scan_id	String	Идентификатор задания на проверку
created	Float	UNIX-время создания сообщения
analysis_duration	Float	Фактическое время поведенческого анализа в секундах
analysis_planned_duration	Float	Планируемое время поведенческого анализа в секундах
correlation_rules_version	String	Версия правил корреляции, которые использовались в ходе поведенческого анализа
detects	Array of strings	Названия вредоносного ПО, обнаруженного в ходе поведенческого анализа
dpi_rules_version	String	Версия правил пакетного анализа трафика, которые использовались в ходе поведенческого анализа
entry_point_id	String	Название источника для проверки, указанное в веб-интерфейсе
entry_point_type	Enum	Тип источника (см. раздел 3.9)
is_from_cache	Boolean	Использовался ли результат предыдущей проверки файла

Поле (объект)	Тип данных	Описание
source_created	Float	UNIX-время создания задания, в котором был проверен файл. Заполняется, если использован результат предыдущей проверки
source_scan_id	String	Идентификатор задания, в котором был проверен файл. Заполняется, если использован результат предыдущей проверки
file	JSON object	Информация о файле
image_info	JSON object	Информация об образе виртуальной машины, который использовался для развертывания виртуальной машины, на которой проводился поведенческий анализ
suspicious_behaviors	Array of JSON objects	Перечень обнаруженного подозрительного поведения
result	JSON object	Итоговый результат поведенческого анализа с его ошибками и состоянием

file

<pre>{ "md5": "<String>", "mime_type": "<String>", "name": "<String>", "sha1": "<String>", "sha256": "<String>", "size": <UInt64> }</pre>		
md5	String	Хеш-сумма файла, вычисленная по алгоритму MD5
mime_type	String	MIME-тип файла
name	String	Имя файла
sha1	String	Хеш-сумма файла, вычисленная по алгоритму SHA-1
sha256	String	Хеш-сумма файла, вычисленная по алгоритму SHA-256
size	UInt64	Размер файла в байтах

Поле (объект)	Тип данных	Описание
image_info		
<pre>{ "name": "<String>", "os": { "architecture": "<String>", "locale": "<String>", "name": "<String>", "service_pack": "<String>", "version": "<String>" }, "version": "<String>" }</pre>		
name	String	Название образа виртуальной машины, который использовался для развертывания виртуальной машины, на которой проводился поведенческий анализ
os	JSON object	Информация об операционной системе образа виртуальной машины
os → architecture	String	Архитектура процессора, которую поддерживает операционная система
os → locale	String	Локаль операционной системы
os → name	String	Название операционной системы
os → service_pack	String	Название пакета обновления операционной системы
os → version	String	Версия операционной системы
version	String	Версия образа виртуальной машины, который использовался для развертывания виртуальной машины, на которой проводился поведенческий анализ
suspicious_behaviors		
<pre>[{ "name": "<String>", "version": "<String>" }]</pre>		
name	String	Внутреннее название обнаруженного подозрительного поведения

Поле (объект)	Тип данных	Описание
version	String	Версия правила, при помощи которого было обнаружено подозрительное поведение
result		
<pre>{ "errors": <JSON object>, "state": "<Enum>", "verdict": <JSON object> }</pre>		
errors	JSON object	Ошибки проверки
state	Enum	Состояние проверки объекта: — UNSCANNED — не проверен из-за ошибки; — PARTIAL — проверен частично; — FULL — проверен
verdict	JSON object	Данные о результате проверки
result → errors		
<pre>{ "corrupted": <Boolean>, "encrypted": <Boolean>, "internal": <Boolean>, "limit_exceeded": <Boolean> }</pre>		
corrupted	Boolean	Файл поврежден
encrypted	Boolean	Файл зашифрован паролем, который неизвестен продукту
internal	Boolean	Внутренняя ошибка при проверке
limit_exceeded	Boolean	Проверка файла остановлена по лимиту (например, превышен максимально допустимый уровень вложенности архивов или максимальный размер файла)

Поле (объект)	Тип данных	Описание
result → verdict		
<pre>{ "accuracy": <Float>, "threat": { "classification": "<Enum>", "family": "<String>", "platform": "<Enum>" }, "threat_level": "<Enum>" }</pre>		
accuracy	Float	Точность результата проверки
threat	JSON object	Информация об обнаруженной угрозе
threat → classification	Enum	Тип обнаруженного вредоносного ПО (см. раздел 3.11)
threat → family	String	Семейство, к которому принадлежит обнаруженное вредоносное ПО
threat → platform	Enum	Семейство операционных систем, на которое нацелено вредоносное ПО: — ANDROID; — IOS; — LINUX; — OSX; — WINDOWS; — NO_PLATFORM — семейство операционных систем не было определено
threat_level	Enum	Результат проверки объекта: — CLEAN — без обнаруженных угроз; — DANGEROUS — опасный; — UNKNOWN — результат неизвестен; — UNWANTED — потенциально опасный

Примеры

Пример сообщения с результатами поведенческого анализа файла:

```
<100>1 2024-01-15T07:22:44.018041Z example-host emailsecurity -
scan_machine.file_result.pt_sandbox - {
  "scan_id": "a36a1f7c-51af-32b1-a144-659b1dfe31c1",
  "created": 1511421763.37285,
  "analysis_duration": 240.0,
  "analysis_planned_duration": 240.0,
  "correlation_rules_version": "1.0.0.524",
  "detects": [
  ],
  "dpi_rules_version": "1.0.0.138",
  "entry_point_id": "example_source_name",
  "entry_point_type": "icap",
  "is_from_cache": true,
  "source_created": 1719808414.6573,
  "source_scan_id": "392e2606-377c-11ef-8002-cfcd208495d5",
  "file": {
    "md5": "11aced0fd6535f6e...1495ba1c7be00",
    "mime_type": "application/x-dosexec; charset=binary",
    "name": "software.exe",
    "sha1": "45e50e2af429e44...6f59e46b18b60",
    "sha256": "23ef04408bb2c...7928e7caf3d7f",
    "size": 33
  },
  "image_info": {
    "name": "win7-sp1-x64",
    "os": {
      "architecture": "x64",
      "locale": "en-US",
      "name": "Windows 7 ENTERPRISE",
      "service_pack": "Service Pack 1",
      "version": "6.1.7601"
    },
    "version": "1.0.0.50"
  },
  "image_name": "win7-sp1-x64",
  "suspicious_behaviors": [
    {
      "name": "Read.System.GetCursorPos.CheckVM",
      "version": ""
    },
    {
      "name": "Read.File.Name.Enumeration",
      "version": ""
    }
  ]
}
```

```

    }
  ],
  "result": {
    "errors": {
      "corrupted": false,
      "encrypted": false,
      "internal": false
    },
    "state": "FULL",
    "verdict": {
      "accuracy": 0.0,
      "threat": {
        "classification": "UNKNOWN",
        "family": "",
        "platform": "NO_PLATFORM"
      },
      "threat_level": "CLEAN"
    }
  }
}

```

3.5.4. Сообщение scan_machine.file_result.melded

Сообщение отправляется при вынесении вердикта по объекту.

Тело сообщения:

```

{
  "scan_id": "<String>",
  "created": <Float>,
  "entry_point_id": "<String>",
  "entry_point_type": "<Enum>",
  "file": <JSON-object> или "url": <JSON-object>
  "result": <JSON-object>
}

```

Таблица 47. Поля сообщения scan_machine.file_result.melded

Поле (объект)	Тип данных	Описание
scan_id	String	Идентификатор задания на проверку
created	Float	UNIX-время создания сообщения
entry_point_id	String	Название источника для проверки, указанное в веб-интерфейсе
entry_point_type	Enum	Тип источника (см. раздел 3.9)
file	JSON-object	Информация о проверяемом файле

Поле (объект)	Тип данных	Описание
url	JSON-object	Информация о проверяемой ссылке
result	JSON-object	Итоговый результат проверки файла с учетом результатов проверки всех дочерних объектов
file		
<pre>{ "md5": "<String>", "mime_type": "<String>", "name": "<String>", "sha1": "<String>", "sha256": "<String>", "size": <UInt64> }</pre>		
md5	String	Хеш-сумма файла, вычисленная по алгоритму MD5
mime_type	String	MIME-тип файла
name	String	Имя файла
sha1	String	Хеш-сумма файла, вычисленная по алгоритму SHA-1
sha256	String	Хеш-сумма файла, вычисленная по алгоритму SHA-256
size	UInt64	Размер файла в байтах
url		
<pre>{ "value": "<String>" }</pre>		
value	String	Ссылка
result		
<pre>{ "errors": <JSON object>, "network_objects": [<JSON-object "domain">, <JSON-object "domain">, <JSON-object "url">, ...], "state": "<Enum>", "verdict": <JSON object> }</pre>		
errors	JSON object	Ошибки проверки

Поле (объект)	Тип данных	Описание
network_objects	Array of JSON-objects	Обнаруженные сетевые объекты: — domain — домен; — ip — IP-адрес; — url — ссылка
state	String	Состояние проверки: — UNSCANNED — файл не был проверен из-за ошибки; — PARTIAL — файл был проверен частично; — FULL — файл был проверен полностью
verdict	JSON object	Вердикт по объекту

result → errors

<pre>{ "corrupted": <Boolean>, "encrypted": <Boolean>, "internal": <Boolean>, "limit_exceeded": <Boolean> }</pre>		
corrupted	Boolean	Файл поврежден
encrypted	Boolean	Файл зашифрован паролем, который неизвестен продукту
internal	Boolean	Внутренняя ошибка при проверке
limit_exceeded	Boolean	Проверка файла остановлена по лимиту (например, превышен максимально допустимый уровень вложенности архивов или максимальный размер файла)

Поле (объект)	Тип данных	Описание
result → network_objects		
<pre>[{ "domain": { "value": "<String>" } }, { "ip": { "value": "<String>" } }, { "url": { "value": "<String>" } }, ...]</pre>		
domain	JSON object	Информация о домене
domain → value	String	Имя домена
ip	JSON object	Информация об IP-адресе
ip → value	String	IP-адрес
url	JSON object	Информация о ссылке
url → value	String	Ссылка
result → verdict		
<pre>{ "accuracy": <Float>, "threat": { "classification": "<Enum>", "family": "<String>", "platform": "<Enum>" }, "threat_level": "<Enum>" }</pre>		
accuracy	Float	Точность результата проверки
threat	JSON object	Информация об обнаруженной угрозе
threat → classification	Enum	Тип обнаруженного вредоносного ПО (см. раздел 3.11)

Поле (объект)	Тип данных	Описание
threat → family	String	Семейство, к которому принадлежит обнаруженное вредоносное ПО
threat → platform	Enum	Семейство операционных систем, на которое нацелено вредоносное ПО: — ANDROID; — IOS; — LINUX; — OSX; — WINDOWS; — NO_PLATFORM — семейство операционных систем не было определено
threat_level	Enum	Результат проверки объекта: — CLEAN — без обнаруженных угроз; — DANGEROUS — опасный; — UNKNOWN — результат неизвестен; — UNWANTED — потенциально опасный

Примеры

Пример сообщения с вердиктом по файлу:

```
<100>1 2024-01-15T07:22:44.018041Z example-host emailsecurity -
scan_machine.file_result.melded - {
  "scan_id": "a36a1f7c-51af-32b1-a144-659b1dfe31c1",
  "created": 1511421763.3728465,
  "entry_point_id": "example_source_name",
  "entry_point_type": "icap",
  "file": {
    "mime_type": "application/x-dosexec; charset=binary",
    "md5": "11aced0fd6535f6e...1495ba1c7be00",
    "name": "software.exe",
    "sha1": "45e50e2af429e44...6f59e46b18b60",
    "sha256": "23ef04408bb2c...7928e7caf3d7f",
    "size": 64000
  },
  "result": {
    "verdict": {
      "threat_level": "CLEAN",
      "threat": {
        "classification": "UNKNOWN",
        "platform": "NO_PLATFORM",
        "family": ""
      },
    },
    "accuracy": 1.0
  },
  "errors": {
    "internal": false,
    "corrupted": false,
    "encrypted": false,
  },
  "state": "FULL"
}
```

3.5.5. Сообщение scan_machine.final_result

Сообщение отправляется при вынесении вердикта по заданию.

Тело сообщения:

```
{
  "scan_id": "<String>",
  "created": <Float>,
  "entry_point_id": "<String>",
  "entry_point_type": "<Enum>",
  "result": <JSON object>
}
```

Таблица 48. Поля сообщения scan_machine.final_result

Поле (объект)	Тип данных	Описание
scan_id	String	Идентификатор задания на проверку
created	Float	UNIX-время создания сообщения
entry_point_id	String	Название источника для проверки, указанное в веб-интерфейсе
entry_point_type	Enum	Тип источника (см. раздел 3.9)
result	JSON object	Итоговый результат проверки задания с учетом результатов проверки всех дочерних объектов

result		
<pre>{ "errors": <JSON object>, "state": "<Enum>", "verdict": <JSON object> }</pre>		
errors	JSON object	Ошибки проверки
state	Enum	Состояние проверки объекта: — UNSCANNED — не проверен из-за ошибки; — PARTIAL — проверен частично; — FULL — проверен
verdict	JSON object	Данные о результате проверки

result → errors		
<pre>{ "corrupted": <Boolean>, "encrypted": <Boolean>, "internal": <Boolean>, "limit_exceeded": <Boolean> }</pre>		

Поле (объект)	Тип данных	Описание
corrupted	Boolean	Файл поврежден
encrypted	Boolean	Файл зашифрован паролем, который неизвестен продукту
internal	Boolean	Внутренняя ошибка при проверке
limit_exceeded	Boolean	Проверка файла остановлена по лимиту (например, превышен максимально допустимый уровень вложенности архивов или максимальный размер файла)

result → verdict

<pre>{ "accuracy": <Float>, "threat": { "classification": "<Enum>", "family": "<String>", "platform": "<Enum>" }, "threat_level": "<Enum>" }</pre>		
accuracy	Float	Точность результата проверки
threat	JSON object	Информация об обнаруженной угрозе
threat → classification	Enum	Тип обнаруженного вредоносного ПО (см. раздел 3.11)
threat → family	String	Семейство, к которому принадлежит обнаруженное вредоносное ПО
threat → platform	Enum	Семейство операционных систем, на которое нацелено вредоносное ПО: — ANDROID; — IOS; — LINUX; — OSX; — WINDOWS; — NO_PLATFORM — семейство операционных систем не было определено
threat_level	Enum	Результат проверки объекта: — CLEAN — без обнаруженных угроз; — DANGEROUS — опасный;

Поле (объект)	Тип данных	Описание
		- UNKNOWN — результат неизвестен; - UNWANTED — потенциально опасный

Примеры

Пример сообщения с вердиктом по заданию:

```
<100>1 2024-01-15T07:22:44.018041Z example-host emailsecurity -
scan_machine.final_result - {
  "scan_id": "a36a1f7c-51af-32b1-a144-659b1dfe31c1",
  "created": 1511421763.37285,
  "entry_point_id": "example_source_name",
  "entry_point_type": "icap",
  "result": {
    "errors": {
      "corrupted": false,
      "encrypted": false,
      "internal": false
    },
    "state": "FULL",
    "verdict": {
      "accuracy": 1.0,
      "threat": {
        "classification": "UNKNOWN",
        "family": "",
        "platform": "NO_PLATFORM"
      },
      "threat_level": "CLEAN"
    }
  },
}
```

3.6. Завершение работы с источником

После выполнения задания PT Email Security принимает решение о блокировке объекта задания и отправляется сообщение о завершении работы с источником. В разделе описаны типы сообщений, которые отправляются для указанных в таблице источников.

Таблица 49. Типы сообщений, регистрируемые при завершении работы с источниками

Тип сообщения	Источник
user_scan.finish	Веб-интерфейс
check_me.finish	Служба Checkme

Тип сообщения	Источник
email.finish	Сервер Microsoft Exchange с установленным агентом
mail_agent_mta.finish	Почтовый шлюз безопасности
mail_bcc.finish	Почтовый сервер в режиме зеркалирования
mail_gateway.finish	Почтовый сервер в режиме фильтрации
mail_gateway_mta.finish	Почтовый сервер в режиме фильтрации (MTA)
files_monitor.finish	Общая папка
files_inbox.finish	Папка-шлюз
icap.finish	ICAP-сервер
dpi.finish	PT NAD
retro.finish	Хранилище файлов (при завершении повторной проверки файлов)
public_api.finish	Публичный API при проверке с передаваемыми параметрами
scan_api.finish	Публичный API при проверке с параметрами источника
pt_edr.finish	MaxPatrol EDR

В этом разделе

[Сообщение user_scan.finish \(см. раздел 3.6.1\)](#)

[Сообщение check_me.finish \(см. раздел 3.6.2\)](#)

[Сообщение email.finish \(см. раздел 3.6.3\)](#)

[Сообщение mail_agent_mta.finish \(см. раздел 3.6.4\)](#)

[Сообщение mail_bcc.finish \(см. раздел 3.6.5\)](#)

[Сообщение mail_gateway.finish \(см. раздел 3.6.6\)](#)

[Сообщение mail_gateway_mta.finish \(см. раздел 3.6.7\)](#)

[Сообщение files_monitor.finish \(см. раздел 3.6.8\)](#)

[Сообщение files_inbox.finish \(см. раздел 3.6.9\)](#)

[Сообщение icap.finish \(см. раздел 3.6.10\)](#)

[Сообщение dpi.finish \(см. раздел 3.6.11\)](#)

[Сообщение retro.finish \(см. раздел 3.6.12\)](#)

[Сообщение public_api.finish \(см. раздел 3.6.13\)](#)

Сообщение `scan_api.finish` (см. раздел 3.6.14)

Сообщение `pt_edr.finish` (см. раздел 3.6.15)

3.6.1. Сообщение `user_scan.finish`

Сообщение отправляется при завершении задания на проверку объекта, полученного через веб-интерфейс.

Тело сообщения:

```
{
  "scan_id": "<String>",
  "created": <Float>,
  "status": "<Enum>"
}
```

Таблица 50. Поля сообщения `user_scan.finish`

Поле (объект)	Тип данных	Описание
<code>scan_id</code>	String	Идентификатор задания на проверку
<code>created</code>	Float	UNIX-время создания сообщения
<code>status</code>	Enum	Статус задания на проверку: — FAIL — завершено с ошибкой; — SUCCESS — успешно завершено; — UNKNOWN — выполняется

Примеры

Пример сообщения при успешном завершении задания на проверку:

```
<100>1 2024-01-15T07:22:44.018041Z example-host emailsecurity - user_scan.finish - {
  "scan_id": "a36a1f7c-51af-32b1-a144-659b1dfe31c1",
  "created": 1511421763.3728465,
  "status": "SUCCESS"
}
```

3.6.2. Сообщение `check_me.finish`

Сообщение отправляется при завершении задания на проверку объекта, полученного службой Checkme.

Тело сообщения:

```
{
  "scan_id": "<String>",
  "created": <Float>,
  "status": "<Enum>"
}
```

Таблица 51. Поля сообщения check_me.finish

Поле (объект)	Тип данных	Описание
scan_id	String	Идентификатор задания на проверку
created	Float	UNIX-время создания сообщения
status	Enum	Статус задания на проверку: — FAIL — завершено с ошибкой; — SUCCESS — успешно завершено; — UNKNOWN — выполняется

Примеры

Пример сообщения при успешном завершении задания на проверку:

```
<100>1 2024-01-15T07:22:44.018041Z example-host emailsecurity - check_me.finish - {
  "scan_id": "a36a1f7c-51af-32b1-a144-659b1dfe31c1",
  "created": 1511421763.3728465,
  "status": "SUCCESS"
}
```

3.6.3. Сообщение email.finish

Сообщение отправляется при завершении задания на проверку письма, полученного почтовым агентом.

Тело сообщения:

```
{
  "scan_id": "<String>",
  "created": <Float>,
  "status": "<Enum>",
  "action": "<Enum>"
}
```

Таблица 52. Поля сообщения email.finish

Поле (объект)	Тип данных	Описание
scan_id	String	Идентификатор задания на проверку
created	Float	UNIX-время создания сообщения
status	Enum	Статус задания на проверку: — FAIL — завершено с ошибкой; — SUCCESS — успешно завершено; — UNKNOWN — выполняется
action	Enum	Решение о блокировке объекта задания: — BLOCK — распространение объекта было заблокировано (только если источник работает в блокирующем режиме); — NOTHING — во время проверки произошла ошибка и объект был пропущен в информационную систему организации; — PASS — объект пропущен в информационную систему организации; — UNKNOWN — действие неизвестно

Примеры

Пример сообщения при успешном завершении задания на проверку:

```
<100>1 2024-01-15T07:22:44.018041Z example-host emailsecurity - email.finish - {
  "scan_id": "a36a1f7c-51af-32b1-a144-659b1dfe31c1",
  "created": 1511421763.37285,
  "status": "SUCCESS",
  "action": "BLOCK"
}
```

3.6.4. Сообщение mail_agent_mta.finish

Сообщение отправляется при завершении задания на проверку письма, полученного от почтового шлюза безопасности.

Тело сообщения:

```
{
  "scan_id": "<String>",
  "created": <Float>,
  "status": "<Enum>",
  "action": "<Enum>"
}
```

Таблица 53. Поля сообщения mail_agent_mta.finish

Поле (объект)	Тип данных	Описание
scan_id	String	Идентификатор задания на проверку
created	Float	UNIX-время создания сообщения
status	Enum	Статус задания на проверку: — FAIL — завершено с ошибкой; — SUCCESS — успешно завершено; — UNKNOWN — выполняется
action	Enum	Решение о блокировке объекта задания: — BLOCK — распространение объекта было заблокировано (только если источник работает в блокирующем режиме); — NOTHING — во время проверки произошла ошибка и объект был пропущен в информационную систему организации; — PASS — объект пропущен в информационную систему организации; — UNKNOWN — действие неизвестно

Примеры

Пример сообщения при успешном завершении задания на проверку:

```
<100>1 2024-01-15T07:22:44.018041Z example-host emailsecurity - mail_agent_mta.finish
- {
  "scan_id": "a36a1f7c-51af-32b1-a144-659b1dfe31c1",
  "created": 1511421763.3728465,
  "status": "SUCCESS",
  "action": "BLOCK"
}
```

3.6.5. Сообщение mail_bcc.finish

Сообщение отправляется при завершении задания на проверку письма, полученного от почтового сервера в виде скрытой копии.

Тело сообщения:

```
{
  "scan_id": "<String>",
  "created": <Float>,
  "status": "<Enum>"
}
```

Таблица 54. Поля сообщения mail_bcc.finish

Поле (объект)	Тип данных	Описание
scan_id	String	Идентификатор задания на проверку
created	Float	UNIX-время создания сообщения
status	Enum	Статус задания на проверку: — FAIL — завершено с ошибкой; — SUCCESS — успешно завершено; — UNKNOWN — выполняется

Примеры

Пример сообщения при успешном завершении задания на проверку:

```
<100>1 2024-01-15T07:22:44.018041Z example-host emailsecurity - mail_bcc.finish - {
  "scan_id": "a36a1f7c-51af-32b1-a144-659b1dfe31c1",
  "created": 1511421763.3728465,
  "status": "SUCCESS"
}
```

3.6.6. Сообщение mail_gateway.finish

Сообщение отправляется при завершении задания на проверку письма, полученного от почтового сервера в режиме фильтрации.

Тело сообщения:

```
{
  "scan_id": "<String>",
  "created": <Float>,
  "status": "<Enum>",
  "action": "<Enum>"
}
```

Таблица 55. Поля сообщения mail_gateway.finish

Поле (объект)	Тип данных	Описание
scan_id	String	Идентификатор задания на проверку
created	Float	UNIX-время создания сообщения
status	Enum	Статус задания на проверку: — FAIL — завершено с ошибкой; — SUCCESS — успешно завершено; — UNKNOWN — выполняется
action	Enum	Решение о блокировке объекта задания: — BLOCK — распространение объекта было заблокировано (только если источник работает в блокирующем режиме); — NOTHING — во время проверки произошла ошибка и объект был пропущен в информационную систему организации; — PASS — объект пропущен в информационную систему организации; — UNKNOWN — действие неизвестно

Примеры

Пример сообщения при успешном завершении задания на проверку:

```
<100>1 2024-01-15T07:22:44.018041Z example-host emailsecurity - mail_gateway.finish -
{
  "scan_id": "a36a1f7c-51af-32b1-a144-659b1dfe31c1",
  "created": 1511421763.3728465,
  "status": "SUCCESS",
  "action": "BLOCK"
}
```

3.6.7. Сообщение mail_gateway_mta.finish

Сообщение отправляется при завершении задания на проверку письма, полученного от почтового сервера в режиме фильтрации (MTA).

Тело сообщения:

```
{
  "scan_id": "<String>",
  "created": <Float>,
  "status": "<Enum>",
  "action": "<Enum>"
}
```

Таблица 56. Поля сообщения mail_gateway_mta.finish

Поле (объект)	Тип данных	Описание
scan_id	String	Идентификатор задания на проверку
created	Float	UNIX-время создания сообщения
status	Enum	Статус задания на проверку: — FAIL — завершено с ошибкой; — SUCCESS — успешно завершено; — UNKNOWN — выполняется
action	Enum	Решение о блокировке объекта задания: — BLOCK — распространение объекта было заблокировано (только если источник работает в блокирующем режиме); — NOTHING — во время проверки произошла ошибка и объект был пропущен в информационную систему организации; — PASS — объект пропущен в информационную систему организации; — UNKNOWN — действие неизвестно

Примеры

Пример сообщения при успешном завершении задания на проверку:

```
<100>1 2024-01-15T07:22:44.018041Z example-host emailsecurity -
mail_gateway_mta.finish - {
  "scan_id": "a36a1f7c-51af-32b1-a144-659b1dfe31c1",
  "created": 1511421763.3728465,
  "status": "SUCCESS",
  "action": "BLOCK"
}
```

3.6.8. Сообщение files_monitor.finish

Сообщение отправляется при завершении задания на проверку объекта из общей папки.

Тело сообщения:

```
{
  "scan_id": "<String>",
  "created": <Float>,
  "status": "<Enum>"
}
```

Таблица 57. Поля сообщения files_monitor.finish

Поле (объект)	Тип данных	Описание
scan_id	String	Идентификатор задания на проверку
created	Float	UNIX-время создания сообщения
status	Enum	Статус задания на проверку: — FAIL — завершено с ошибкой; — SUCCESS — успешно завершено; — UNKNOWN — выполняется

Примеры

Пример сообщения при успешном завершении задания на проверку:

```
<100>1 2024-01-15T07:22:44.018041Z example-host emailsecurity - files_monitor.finish
- {
  "scan_id": "a36a1f7c-51af-32b1-a144-659b1dfe31c1",
  "created": 1511421763.3728465,
  "status": "SUCCESS"
}
```

3.6.9. Сообщение files_inbox.finish

Сообщение отправляется при завершении задания на проверку объекта, добавленного в папку-шлюз.

Тело сообщения:

```
{
  "scan_id": "<String>",
  "created": <Float>,
  "status": "<Enum>",
  "action": "<Enum>",
  "dst_file_info": <JSON object>
}
```

Таблица 58. Поля сообщения files_inbox.finish

Поле (объект)	Тип данных	Описание
scan_id	String	Идентификатор задания на проверку
created	Float	UNIX-время создания сообщения
status	Enum	Статус задания на проверку: — FAIL — завершено с ошибкой; — SUCCESS — успешно завершено; — UNKNOWN — выполняется
action	Enum	Решение о блокировке объекта задания: — BLOCK — распространение объекта было заблокировано (только если источник работает в блокирующем режиме); — NOTHING — во время проверки произошла ошибка и объект был пропущен в информационную систему организации; — PASS — объект пропущен в информационную систему организации; — UNKNOWN — действие неизвестно
dst_file_info	JSON object	Информация о перемещенном файле
dst_file_info → url	String	Путь к перемещенному файлу в папке для безопасных файлов или в папке карантина

Примеры

Пример сообщения при успешном завершении задания на проверку:

```
<100>1 2024-01-15T07:22:44.018041Z example-host emailsecurity - files_inbox.finish -
{
  "scan_id": "a36a1f7c-51af-32b1-a144-659b1dfe31c1",
  "created": 1511421763.3728465,
  "status": "SUCCESS",
  "action": "NOTHING",
  "dst_file_info": {
    "url": "smb://host/share/safe/software.exe"
  }
}
```

3.6.10. Сообщение icap.finish

Сообщение отправляется при завершении задания на проверку контента, полученного по ICAP.

Тело сообщения:

```
{
  "scan_id": "<String>",
  "created": <Float>,
  "status": "<Enum>",
  "action": "<Enum>"
}
```

Таблица 59. Поля сообщения icap.finish

Поле (объект)	Тип данных	Описание
scan_id	String	Идентификатор задания на проверку
created	Float	UNIX-время создания сообщения
status	Enum	Статус задания на проверку: — FAIL — завершено с ошибкой; — SUCCESS — успешно завершено; — UNKNOWN — выполняется

Поле (объект)	Тип данных	Описание
action	Enum	Решение о блокировке объекта задания: — BLOCK — распространение объекта было заблокировано (только если источник работает в блокирующем режиме); — NOTHING — во время проверки произошла ошибка и объект был пропущен в информационную систему организации; — PASS — объект пропущен в информационную систему организации; — UNKNOWN — действие неизвестно

Примеры

Пример сообщения при успешном завершении задания на проверку:

```
<100>1 2024-01-15T07:22:44.018041Z example-host emailsecurity - icap.finish - {
  "scan_id": "a36a1f7c-51af-32b1-a144-659b1dfe31c1",
  "created": 1511421763.3728465,
  "status": "SUCCESS",
  "action": "BLOCK"
}
```

3.6.11. Сообщение dpi.finish

Сообщение отправляется при завершении задания на проверку файла, полученного от PT NAD.

Тело сообщения:

```
{
  "scan_id": "<String>",
  "created": <Float>,
  "status": "<Enum>"
}
```

Таблица 60. Поля сообщения dpi.finish

Поле (объект)	Тип данных	Описание
scan_id	String	Идентификатор задания на проверку
created	Float	UNIX-время создания сообщения

Поле (объект)	Тип данных	Описание
status	Enum	Статус задания на проверку: — FAIL — завершено с ошибкой; — SUCCESS — успешно завершено; — UNKNOWN — выполняется

Примеры

Пример сообщения при успешном завершении задания на проверку:

```
<100>1 2024-01-15T07:22:44.018041Z example-host emailsecurity - dpi.finish - {
  "scan_id": "a36a1f7c-51af-32b1-a144-659b1dfe31c1",
  "created": 1511421763.3728465,
  "status": "SUCCESS"
}
```

3.6.12. Сообщение retro.finish

Сообщение отправляется при завершении задания на повторную проверку файлов в хранилище.

Тело сообщения:

```
{
  "scan_id": "<String>",
  "created": <Float>,
  "status": "<Enum>"
}
```

Таблица 61. Поля сообщения retro.finish

Поле (объект)	Тип данных	Описание
scan_id	String	Идентификатор задания на проверку
created	Float	UNIX-время создания сообщения
status	Enum	Статус задания на проверку: — FAIL — завершено с ошибкой; — SUCCESS — успешно завершено; — UNKNOWN — выполняется

Примеры

Пример сообщения при успешном завершении задания на проверку:

```
<100>1 2024-01-15T07:22:44.018041Z example-host emailsecurity - retro.finish - {
  "scan_id": "a36a1f7c-51af-32b1-a144-659b1dfe31c1",
  "created": 1511421763.3728465,
  "status": "SUCCESS"
}
```

3.6.13. Сообщение public_api.finish

Сообщение отправляется при завершении задания на проверку объекта, полученного от сервиса публичного API при проверке с передаваемыми параметрами.

Тело сообщения:

```
{
  "scan_id": "<String>",
  "created": <Float>,
  "status": "<Enum>"
}
```

Таблица 62. Поля сообщения public_api.finish

Поле (объект)	Тип данных	Описание
scan_id	String	Идентификатор задания на проверку
created	Float	UNIX-время создания сообщения
status	Enum	Статус задания на проверку: — FAIL — завершено с ошибкой; — SUCCESS — успешно завершено; — UNKNOWN — выполняется

Примеры

Пример сообщения при успешном завершении задания на проверку:

```
<100>1 2024-01-15T07:22:44.018041Z example-host emailsecurity - public_api.finish - {
  "scan_id": "a36a1f7c-51af-32b1-a144-659b1dfe31c1",
  "created": 1511421763.3728465,
  "status": "SUCCESS"
}
```

3.6.14. Сообщение scan_api.finish

Сообщение отправляется при завершении задания на проверку объекта, полученного от сервиса публичного API при проверке с параметрами источника.

Тело сообщения:

```
{
  "scan_id": "<String>",
  "created": <Float>,
  "status": "<Enum>"
}
```

Таблица 63. Поля сообщения scan_api.finish

Поле (объект)	Тип данных	Описание
scan_id	String	Идентификатор задания на проверку
created	Float	UNIX-время создания сообщения
status	Enum	Статус задания на проверку: — FAIL — завершено с ошибкой; — SUCCESS — успешно завершено; — UNKNOWN — выполняется

Примеры

Пример сообщения при успешном завершении задания на проверку:

```
<100>1 2024-01-15T07:22:44.018041Z example-host emailsecurity - scan_api.finish - {
  "scan_id": "a36a1f7c-51af-32b1-a144-659b1dfe31c1",
  "created": 1511421763.3728465,
  "status": "SUCCESS"
}
```

3.6.15. Сообщение pt_edr.finish

Сообщение отправляется при завершении задания на проверку файлов конечных устройств, полученных от источника MaxPatrol EDR.

Тело сообщения:

```
{
  "scan_id": "<String>",
  "created": <Float>,
  "status": "<Enum>"
}
```

Таблица 64. Поля сообщения pt_edr.finish

Поле (объект)	Тип данных	Описание
scan_id	String	Идентификатор задания на проверку
created	Float	UNIX-время создания сообщения
status	Enum	Статус задания на проверку: — FAIL — завершено с ошибкой; — SUCCESS — успешно завершено; — UNKNOWN — выполняется

Примеры

Пример сообщения при успешном завершении задания на проверку:

```
<100>1 2024-01-15T07:22:44.018041Z example-host emailsecurity - pt_edr.finish - {
  "scan_id": "a36a1f7c-51af-32b1-a144-659b1dfe31c1",
  "created": 1511421763.3728465,
  "status": "SUCCESS"
}
```

3.7. Обновление средства проверки, av.update

Сообщение отправляется при обновлении средств проверки, антивирусов и их баз.

Тело сообщения:

```
{
  "av_code_name": "<String>",
  "created": <Float>,
  "database_time": <Float>,
  "engine_version": "<String>"
}
```

Таблица 65. Поля сообщения av.update

Поле (объект)	Тип данных	Описание
av_code_name	String	Название средства проверки (см. раздел 3.10)
created	Float	UNIX-время создания сообщения
database_time	Float	UNIX-время выпуска базы
engine_version	String	Версия средства проверки

Примеры

Пример сообщения при обновлении антивируса ClamAV:

```
<100>1 2024-01-15T07:22:44.018041Z example-host emailsecurity - av.update - {
  "created": 1520866088.3110101,
  "av_code_name": "clamav",
  "engine_version": "11.0.1.22",
  "database_time": 1520862339.0
}
```

3.8. События аудита, audit.event

Сообщение отправляется при регистрации каждого события аудита пользователей PT Email Security.

Тело сообщения:

```
{
  "action": "<Enum>",
  "details": <JSON-object>,
  "domain": "<Enum>",
  "errors": [
    <JSON-object>
  ],
  "id": "<UUID>",
  "name": "<Enum>",
  "object_id": "<String>",
  "status": "<Enum>",
  "subdomain": "<Enum>",
  "text": "<String>",
  "time": <Float>,
  "user_id": "<UUID>",
  "user_login": "<String>"
}
```

Таблица 66. Поля сообщения audit.event

Поле (объект)	Тип данных	Описание
action	Enum	Действие: — CREATE — создание; — DELETE — удаление; — EXPORT — экспорт; — IMPORT — импорт; — LOGOUT — выход;

Поле (объект)	Тип данных	Описание
		— READ — просмотр; — UPDATE — изменение
details	JSON object	Детали события. Структура JSON-объекта зависит от типа события (не описывается в документации)
domain	Enum	Категория события: — CONFIGURATION — параметры; — DATA — данные; — SECURITY — безопасность
errors	JSON object	Ошибки
id	UUID	Идентификатор события
name	Enum	Тип события (возможные значения указаны в таблице ниже)
object_id	String	Идентификатор объекта зависит от типа объекта: — EMAIL — идентификатор задания; если письмо из карантина — <code>Quarantined emails</code>. — ENTRY_POINT — название источника; если событие связано со сменой режима работы источника — <code>Mail gateway</code>. — FILE — хеш-сумма файла SHA-256. — LOG_FILES — <code>Application logs</code>. — SYSTEM — в зависимости от типа события: <code>Application</code>, <code>License</code> или <code>Settings</code>. — TASK — идентификатор задания; если событие связано с очередью файлов на поведенческий анализ — <code>BaTasks</code>. — TOKEN — название токена доступа; если событие связано с выпуском токена для Grafana — <code>Monitoring token</code>. — SCAN_ENGINE — в зависимости от средства проверки, с которым связано событие: • если событие связано с антивирусом — <code>AV scanner.<Название></code>; • если со средством проверки по YARA-правилам — <code>AV scanner.yara-engine</code>;

Поле (объект)	Тип данных	Описание
		- если с черным или белым списком — Blacklist, Blacklist & Whitelist, Whitelist; - если с другим средством проверки — ptcategorizer, ptesc, ptios или trace2ML
status	Enum	Результат действия: - SUCCESS — успех; - FAILURE — отказ
subdomain	Enum	Тип объекта: - EMAIL — письмо; - ENTRY_POINT — источник; - FILE — файл; - LOG_FILES — журнал; - SCAN_ENGINE — средство проверки; - SYSTEM — параметр PT Email Security; - TASK — задание; - TOKEN — токен доступа
text	String	Описание события
time	Float	Время регистрации события
user_id	UUID	Идентификатор пользователя
user_login	String	Логин пользователя

Значения полей name, subdomain и action для различных типов событий аудита PT Email Security приведены в таблице. Типы событий сгруппированы по значениям поля domain.

Таблица 67. Типы событий аудита по категориям

name	subdomain	action	Описание
Параметры (CONFIGURATION)			
AuditEventEntryPointCreate	ENTRY_POINT	CREATE	Добавление источника
AuditEventEntryPointDelete	ENTRY_POINT	DELETE	Удаление источника
AuditEventEntryPointUpdate	ENTRY_POINT	UPDATE	Изменение параметров источника

name	subdomain	action	Описание
AuditEventMailGWDowngradeMode	ENTRY_POINT	UPDATE	Изменение режима проверки источника с блокирующего на пассивный
AuditEventMailGWUpgradeMode	ENTRY_POINT	UPDATE	Изменение режима проверки источника с пассивного на блокирующий
AuditEventAntivirusCreate	SCAN_ENGINE	CREATE	Установка антивируса
AuditEventAntivirusDelete	SCAN_ENGINE	DELETE	Удаление антивируса
AuditEventAntivirusSettingsUpdate	SCAN_ENGINE	UPDATE	Изменение параметров антивируса
AuditEventBWListAdd	SCAN_ENGINE	CREATE	Добавление записей в черный или белый список
AuditEventBWListDelete	SCAN_ENGINE	DELETE	Удаление записей из черного или белого списка
AuditEventBWListDeleteAll	SCAN_ENGINE	DELETE	Очистка черного или белого списка
AuditEventBWListExport	SCAN_ENGINE	EXPORT	Экспорт записей из черного или белого списка
AuditEventBWListImport	SCAN_ENGINE	CREATE	Импорт записей в черный или белый список
AuditEventBWListRead	SCAN_ENGINE	READ	Просмотр записей в черном или белом списке
AuditEventBWListUpdate	SCAN_ENGINE	UPDATE	Добавление или удаление записей из черного или белого списка
AuditEventInternalEngineSettingsUpdate	SCAN_ENGINE	UPDATE	Изменение параметров антивируса или средства проверки Positive Technologies
AuditEventScanEngineDBUpdate	SCAN_ENGINE	UPDATE	Обновление антивирусной базы или базы знаний средства проверки Positive Technologies
AuditEventYaraEngineRuleDownload	SCAN_ENGINE	EXPORT	Скачивание файла пакета YARA-правил
AuditEventYaraEngineRuleUpload	SCAN_ENGINE	IMPORT	Загрузка файла пакета YARA-правил

name	subdomain	action	Описание
AuditEventYaraEngineSettingsGet	SCAN_ENGINE	READ	Просмотр параметров средства проверки по пользовательским YARA-правилам
AuditEventYaraEngineSettingsSet	SCAN_ENGINE	UPDATE	Изменение параметров средства проверки по пользовательским YARA-правилам
AuditEventYaraEngineSettingsUpdate	SCAN_ENGINE	UPDATE	Включение или отключение средства проверки по пользовательским YARA-правилам
AuditEventAutoUpdateSettingsUpdate	SYSTEM	UPDATE	Изменение параметров обновления PT Email Security
AuditEventBASystemSettingsUpdate	SYSTEM	UPDATE	Изменение правил поведенческого анализа для источников
AuditEventLicenseReplace	SYSTEM	DELETE	Замена лицензии PT Email Security
AuditEventSystemAutoUpdate	SYSTEM	UPDATE	Автоматический запуск обновления PT Email Security
AuditEventSystemManualUpdate	SYSTEM	UPDATE	Ручной запуск обновления PT Email Security
AuditEventSystemSettingsUpdate	SYSTEM	UPDATE	Изменение основных параметров PT Email Security

Данные (DATA)

AuditEventEmailBodyGet	EMAIL	READ	Просмотр тела письма
AuditEventMTAEmailInfoRead	EMAIL	READ	Просмотр информации о письме
AuditEventMTAEmailListRead	EMAIL	READ	Просмотр списка писем
AuditEventQuarantinedMailComment	EMAIL	UPDATE	Добавление комментария к письму в карантине
AuditEventQuarantinedMailForward	EMAIL	UPDATE	Переадресация письма из карантина
AuditEventQuarantinedMailManualDelete	EMAIL	UPDATE	Удаление письма из карантина
AuditEventQuarantinedMailProcess	EMAIL	UPDATE	Изменение информации о письме в карантине

name	subdomain	action	Описание
AuditEventQuarantinedMailRead	EMAIL	READ	Просмотр письма в карантине
AuditEventQuarantinedMailReadList	EMAIL	READ	Просмотр списка писем в карантине
AuditEventQuarantinedMailSend	EMAIL	UPDATE	Выпуск письма из карантина
AuditEventFileDownload	FILE	EXPORT	Скачивание файлов из хранилища
AuditEventSystemLogsDownload	LOG_FILES	EXPORT	Скачивание файлов журналов PT Email Security
AuditEventSandboxLogsDownload	LOG_FILES	EXPORT	Скачивание результатов поведенческого анализа
AuditEventBAScanCreate	TASK	CREATE	Запуск поведенческого анализа файла в интерактивном режиме или с помощью командной строки
AuditEventBATasksCancel	TASK	UPDATE	Отмена поведенческого анализа файла до его начала
AuditEventBATasksChangePriority	TASK	UPDATE	Изменение правила определения приоритета файлов в очереди на поведенческий анализ
AuditEventBATasksChangeRelativePriority	TASK	UPDATE	Изменение приоритета файлов в очереди на поведенческий анализ
AuditEventBATasksList	TASK	READ	Просмотр очереди файлов на поведенческий анализ
AuditEventTasksArtifactsExport	TASK	EXPORT	Скачивание архива с файлами задания
AuditEventTasksRead	TASK	READ	Просмотр задания
Безопасность (SECURITY)			
AuditEventAuthLogout	SYSTEM	LOGOUT	Автоматический выход из PT Email Security из-за неактивности пользователя
AuditEventMonitoringTokenCreate	TOKEN	CREATE	Создание токена доступа для Grafana

name	subdomain	action	Описание
AuditEventTokenAssignToEntryPoint	TOKEN	UPDATE	Привязка токена доступа к источнику
AuditEventTokenBlock	TOKEN	DELETE	Отзыв токена доступа
AuditEventTokenCreate	TOKEN	CREATE	Создание токена доступа
AuditEventTokenUpdate	TOKEN	UPDATE	Изменение комментария к токenu доступа

Примеры

Пример сообщения при обновлении антивирусной базы ClamAV:

```
<100>1 2024-01-15T07:22:44.018041Z example-host emailsecurity - audit.event - {
  "action": "UPDATE",
  "details": {
    "version": "1.0.170.92246"
  },
  "domain": "CONFIGURATION",
  "errors": [
  ],
  "id": "ab761dcc-5575-11f0-8000-32356d16f20c",
  "name": "AuditEventScanEngineDBUpdate",
  "object_id": "AV scanner.clamav",
  "status": "SUCCESS",
  "subdomain": "SCAN_ENGINE",
  "text": "Scan engine db updated",
  "time": 1751262432.0,
  "user_id": "00000000-0000-0000-0000-000000000000",
  "user_login": "system"
}
```

Пример сообщения при просмотре пользователем записей в черном списке:

```
<100>1 2024-01-15T07:22:44.018041Z example-host emailsecurity - audit.event - {
  "action": "READ",
  "details": {
  },
  "domain": "CONFIGURATION",
  "errors": [
  ],
  "id": "2a09712b-5584-11f0-8000-725aa0d6539b",
  "name": "AuditEventBWListRead",
  "object_id": "Blacklist",
  "status": "SUCCESS",
  "subdomain": "SCAN_ENGINE",
  "text": "Read black-white list",
}
```

```

"time": 1751268657.789,
"user_id": "9f59bb78-9804-4b35-95e9-60968f56e3d6",
"user_login": "Ivanov"
}

```

3.9. Типы источников

В таблице указаны возможные значения полей с типом источника.

Таблица 68. Типы источников

Значение	Тип
check_me	Служба Checkme
file_inbox	Папка-шлюз
file_monitor	Общая папка
icap	ICAP-сервер
mail_agent	Сервер Microsoft Exchange с установленным агентом
mail_agent_mta	Почтовый шлюз безопасности
mail_bcc	Почтовый сервер в режиме зеркалирования
mail_gateway	Почтовый сервер в режиме фильтрации
mail_gateway_mta	Почтовый сервер в режиме фильтрации (MTA)
ptedr	MaxPatrol EDR
ptnad	PT NAD
public_api	API с передаваемыми параметрами проверки
retro	Хранилище файлов (ретроспективный анализ)
scan_api	API с выбранными параметрами проверки
web	Веб-интерфейс

3.10. Средства проверки

В таблице указаны возможные значения полей с названиями средств проверки.

Таблица 69. Средства проверки

Значение	Средство проверки
antiphishing	Средство обнаружения угроз в почте PT Anti-Phishing and Anti-Spam
avast	Дополнительный антивирус Avast Core Security
clamav	Антивирус ClamAV

Значение	Средство проверки
kaspersky	Дополнительный антивирус Kaspersky Web Traffic Security
ptav	Антивирус PT AV
ptesc	Средство статического анализа на основе YARA-правил PT ESC
ptioc	Средство обнаружения индикаторов компрометации PT IoC
rule_engine	Пользовательские правила определения объектов с угрозами
vba	Антивирус VBA32

3.11. Типы вредоносного ПО

В таблице указаны возможные значения полей для классификации вредоносного ПО по типам.

Таблица 70. Типы вредоносного ПО

Значение	Тип	Описание
ADWARE	Рекламное ПО	Программное обеспечение, распространяемое в рекламных целях. Незаметно попав на устройство, оно демонстрирует пользователю рекламу, а также собирает пользовательскую информацию для партнерских программ. Может вводить владельца устройства в заблуждение для легитимизации своего присутствия
BACKDOOR	Бэкдор	Вредоносное ПО для скрытого удаленного управления устройством. Представители этого класса — неотъемлемая часть целевых атак
BOOTKIT	Буткит	Вредоносное ПО, запускающее вредоносный код на самых ранних этапах загрузки ОС
CLIENT_IRC	IRC-клиент	Программа, используемая для коммуникации в IRC (Internet Relay Chat), обмена файлами и управляющими командами с применением нестандартного протокола связи. Не является вредоносной, но может быть использована злоумышленниками
CLIENT_P2P	P2P-клиент	Программа, используемая для работы с peer-to-peer-сетями. Применяется для обмена информацией в распределенной архитектуре хранения и передачи данных. Не является вредоносной, но может быть использована злоумышленниками

Значение	Тип	Описание
CLIENT_SMTP	SMTP-клиент	Программа, используемая для отправки электронных писем в скрытом режиме. Чаще применяется в составе многофункционального ПО. Не является вредоносной, но может быть использована злоумышленниками
CONSTRUCTOR	Конструктор	Программа для сборки новых образцов вредоносного ПО. Злоумышленники используют ее при подготовке к атаке. Продается на теневых форумах
DIALER	Средство дозвона	Программа, используемая для установки телефонных соединений в скрытом режиме. Не является вредоносной, но может быть использована злоумышленниками
DOS	DoS-утилита	Программа для проведения атаки типа «отказ в обслуживании». При отправке большого числа запросов принимающая сторона не успевает их обработать и становится временно недоступной. Может использоваться для выведения из строя средств защиты
DOWNLOADER	Загрузчик	Программа для скрытого скачивания данных из сетевых источников. Чаще применяется в составе многофункционального ПО. Не является вредоносной, но может быть использована злоумышленниками
EMAIL_FLOODER	Почтовый спамер	Программа для отправки большого количества бесполезной информации с помощью электронной почты. Может быть использована для рассылки спама, отвлечения внимания пользователя или обхода средств защиты
EMAIL_WORM	Почтовый червь	Вредоносное ПО, способное распространяться с помощью электронных писем
EXPLOIT	Эксплойт	Вредоносное ПО, использующее для развития атаки одну или несколько уязвимостей в целевом ПО. Применяется для запуска вредоносного кода без участия пользователя. Злоумышленники могут использовать его для повышения привилегий на устройстве
FLOODER	Флудильщик	Программа для отправки большого количества бесполезной информации по сетевым каналам. Может быть использована для рассылки спама, отвлечения внимания пользователя или обхода средств защиты
FRAUDTOOL	Инструмент для мошенничества	Программа, которая не выполняет заявленных функций. Может отвлекать пользователя или вводить его в заблуждение. Не является вредоносной, но может быть использована злоумышленниками

Значение	Тип	Описание
HACKTOOL	Пентест-инструменты	Инструмент, помогающий злоумышленнику развить атаку. Может использоваться для изменения параметров устройства, чтобы ослабить его защищенность, или для сокрытия действий атакующего. Применяется в тестировании на проникновение
HOAX	Программа-розыгрыш	Программа, предназначенная для демонстрации пользователю ложной, пугающей информации. Может злоупотреблять ресурсами ОС, причиняя неудобства и побуждая владельца устройства к необдуманным действиям (чаще всего злоумышленники используют такое ПО, чтобы обманом получить деньги пользователя)
IM_FLOODER	IM-флудильщик	Программа для отправки большого количества бесполезной информации через мессенджеры. Может быть использована для рассылки спама, отвлечения внимания пользователя или обхода средств защиты
IM_WORM	IM-червь	Вредоносное ПО, способное распространяться через мессенджеры
IRC_WORM	IRC-червь	Вредоносное ПО, способное распространяться через IRC (Internet Relay Chat)
MONITOR	Средство мониторинга	Программа для наблюдения за действиями пользователя. Применяется для трассировки активности ОС. Не является вредоносной, но может быть использована злоумышленниками
NET_WORM	Сетевой червь	Вредоносное ПО, способное распространяться без участия пользователя. Для этого используются уязвимости в ПО на новых узлах сети с последующим запуском вредоносного кода
NETTOOL	Сетевая утилита	Инструмент, выполняющий действия над сетевыми ресурсами в IT-инфраструктуре. Не является вредоносным ПО, чаще всего используется для сетевого администрирования, но злоумышленники могут применять его для развития атак
P2P_WORM	P2P-червь	Вредоносное ПО, способное распространяться через пиринговые сети
PHISHING	Фишинг	Рассылка с вредоносным содержанием, распространяемая через электронные письма или сообщения в мессенджерах. Злоумышленник обманным путем заставляет пользователя открыть присланный файл или

Значение	Тип	Описание
		перейти по ссылке. Если цель фишинга — кража средств, текст сообщения может содержать побуждение к выполнению денежных операций
PSWTOOL	Средство восстановления паролей	Программа для получения учетных данных пользователя и восстановления утраченной информации. Не является вредоносной, но может быть использована злоумышленниками
REMOTEADMIN	Средство удаленного доступа	Программа для удаленного управления устройством. Применяется для демонстрации действия пользователя или оказания услуг технической поддержки. Не является вредоносной, но может быть использована злоумышленниками
RISKTOOL	Потенциально нежелательное ПО	Инструмент для работы с локальными ресурсами устройства пользователя. Не является вредоносным ПО и чаще всего применяется для администрирования ОС, но, попав в руки злоумышленников, может нанести вред пользовательским данным
ROOTKIT	Руткит	Вредоносное ПО для сокрытия в системе объектов либо действий злоумышленника
SERVER_FTP	FTP-сервер	Удаленный компьютер, выполняющий функции FTP-сервера. Применяется для получения удаленного доступа к хранилищу данных на устройстве. Не является вредоносным ПО, но может быть использован злоумышленниками
SERVER_PROXY	Прокси-сервер	Удаленный компьютер, выполняющий функции прокси-сервера. Применяется для передачи данных через промежуточные узлы, когда пользователю нужно оставаться анонимным или отсутствует доступ к какой-либо сети. Не является вредоносным ПО, но может быть использован злоумышленниками
SERVER_TELNET	Telnet-сервер	Удаленный компьютер, выполняющий функции Telnet-сервера. Применяется для получения удаленного доступа к устройству пользователя. Не является вредоносным ПО, но может быть использован злоумышленниками
SERVER_WEB	Веб-сервер	Удаленный компьютер, выполняющий функции веб-сервера. Применяется для назначения устройству роли управляющего узла либо для получения доступа к информации. Не является вредоносным ПО, но может быть использован злоумышленниками

Значение	Тип	Описание
SMS_FLOODER	СМС-флудильщик	Программа для отправки большого количества бесполезной информации через SMS-сообщения. Может быть использована для рассылки спама, отвлечения внимания пользователя или обхода средств защиты
SPAM	Спам	Электронное письмо в составе массовой рассылки. Чаще всего содержит рекламное сообщение. Не несет ценной информации для пользователя
SPOOFER	Подмена	Программа для подмены идентификатора отправителя при отправке сетевых запросов. Применяется, чтобы скрыть адрес атакующего, помочь ему избежать обнаружения или легитимизировать выполняемые действия
TROJAN	Троян	Вредоносное ПО для совершения нелегитимных действий на устройстве пользователя (их невозможно классифицировать более точно). Не имеет возможностей для самораспространения
TROJAN_ARCBOMB	Архивная бомба	Вредоносное ПО, представляющее собой архив, при распаковке которого большая доля свободного пространства жесткого диска заполняется бесполезными или пустыми данными. Это может привести к замедлению работы устройства или к прекращению работы некоторых программ
TROJAN_BANKER	Банковский троян	Вредоносное ПО для кражи учетных данных пользователя, связанных с финансовыми системами, и передачи полученной информации злоумышленнику
TROJAN_CLICKER	Троян-кликер	Вредоносное ПО, симулирующее обращения к интернет-ресурсам. Используется для искусственной накрутки счетчиков посещений сайта с целью продвижения ресурса либо монетизации
TROJAN_DDOS	DDoS-бот	Вредоносное ПО для проведения распределенных атак типа «отказ в обслуживании». Компьютер пользователя автоматически становится звеном атаки. Злоумышленники могут настраивать ПО, чтобы изменить перечень целевых ресурсов
TROJAN_DOWNLOADER	Загрузчик ВПО	Вредоносное ПО для скачивания и запуска другого вредоносного ПО. Наиболее часто используемый класс вредоносного ПО для первичного заражения устройства

Значение	Тип	Описание
TROJAN_DROPPER	Установщик ВПО	Вредоносное ПО, извлекающее из своего тела и запускающее другое вредоносное ПО. Зачастую такая программа может установить вредоносное ПО нескольких классов
TROJAN_FAKEAV	Лжеанти-вирус	Вредоносное ПО, представляемое пользователю в качестве антивирусного продукта, но не являющееся таковым. Может требовать плату за использование, блокировать работу устройства, нарушать функционирование системы
TROJAN_GAMETHIEF	Средство кражи игровых учетных данных	Вредоносное ПО для кражи пользовательских данных в компьютерных и мобильных играх и передачи полученной информации злоумышленнику
TROJAN_IM	Средство кражи учетных данных мессенджеров	Вредоносное ПО для кражи пользовательских данных в мессенджерах и передачи полученной информации злоумышленнику
TROJAN_MAILFINDER	Сборщик адресов электронной почты	Вредоносное ПО для сбора адресов электронной почты с устройства пользователя и передачи их злоумышленнику
TROJAN_NOTIFIER	Троян-уведомитель	Вредоносное ПО, уведомляющее злоумышленника об успешном заражении устройства. Не получает от злоумышленника дополнительных компонентов или команд
TROJAN_PROXY	Троян-прокси	Вредоносное ПО, предоставляющее злоумышленнику анонимный доступ в интернет через устройство пользователя либо туннелирующее сетевой трафик до недоступных извне узлов сети. Часто используется на стадии горизонтального перемещения либо для извлечения важных данных при проведении атак
TROJAN_PSW	Средство кражи учетных данных	Вредоносное ПО для кражи учетных данных пользователя в системе или других программах и передачи полученной информации злоумышленнику
TROJAN_RANSOM	Троян-вымогатель	Вредоносное ПО для вымогательской деятельности. Ценные файлы владельца устройства шифруются, а за их восстановление предлагается заплатить выкуп. В

Значение	Тип	Описание
		некоторых случаях те же файлы передаются злоумышленнику, чтобы усилить давление на пользователя и повисить шанс оплаты
TROJAN_SMS	СМС-тро- ян	Вредоносное ПО для отправки SMS-сообщений на номера, которые определяет злоумышленник. Может использоваться для подписки пользователя на платные сервисы
TROJAN_SPY	Програм- ма-шпион	Вредоносное ПО для отслеживания действий пользователя (перехват нажатых клавиш на клавиатуре, получение изображения экрана, истории используемых программ, аудиозапись разговоров) и передачи полученной информации злоумышленнику
UNKNOWN	—	Угроз не обнаружено
UNKNOWN_THREAT	—	Тип вредоносного ПО не указан
VIRTOOL	ПО для со- здания ви- русов	Программа, которую злоумышленники используют для модификации вредоносного ПО, чтобы скрыть его от средств защиты. Применяются методы обфускации кода, шифрования данных или стеганографии. Может использоваться для заражения легитимного ПО
VIRUS	Вирус	Вредоносное ПО, способное распространяться среди локальных ресурсов пользователя
WEBTOOLBAR	Панель инструмен- тов браузе- ра	Панель инструментов, расширяющая возможности браузера. Иногда может получать доступ к значимым данным пользователя либо добавлять нежелательные возможности. Не является вредоносным ПО, но может быть использована злоумышленниками
WORM	Компью- терный червь	Вредоносное ПО, способное распространяться среди сетевых ресурсов пользователя

4. Создание пользовательского образа VM

Образы VM используются в PT Email Security для поведенческого анализа файлов в изолированных ОС. Для создания и настройки пользовательских образов VM предназначена утилита ImageBuilder. С помощью утилиты вы можете:

- Создать образ VM Windows из ISO-файла с установочным образом ОС.
- Создать образ VM Windows из готового образа ОС в формате QCOW2.
- Скопировать и настроить образ VM, уже добавленный в PT Email Security.

Утилита ImageBuilder представляет собой приложение для работы из командной строки. Исполняемый файл утилиты вы можете найти на узлах PT Email Security с функцией поведенческого анализа в каталоге `/opt/ptms/sbin/`.

При создании и копировании образа VM утилита ImageBuilder обеспечивает доступ к локальной сети, что упрощает настройку ОС на образе VM и установку дополнительного ПО.

Для доступа к внешним ресурсам утилита ImageBuilder использует параметры прокси-сервера, указанные в переменных окружения `http_proxy`, `https_proxy`, `HTTP_PROXY` или `HTTPS_PROXY`.

Примечание. При возникновении проблем с утилитой ImageBuilder, отправьте в техническую поддержку Positive Technologies файл журнала `imagebuilder.log`, расположенный в каталоге утилиты.

Программные требования

К настройке узла для запуска утилиты ImageBuilder выдвигаются следующие требования:

- Установлен гипервизора Xen и компоненты PT Email Security.
- Установлена программа `sudo`. Пользователь добавлен в группу `sudo`.
- Установлен VNC-сервер.
- Разрешено подключение к VNC-серверу через порт 8081 (или другой порт, указанный при запуске сервера).
- Обеспечен доступ к сайту msdl.microsoft.com (при подключении используется протокол HTTP и порт 80).

В этом разделе

[Установка и настройка VNC-сервера \(см. раздел 4.1\)](#)

[Создание образа VM из ISO-файла \(см. раздел 4.2\)](#)

[Создание образа VM из образа диска в формате QCOW2 \(см. раздел 4.3\)](#)

[Копирование добавленного ранее образа VM \(см. раздел 4.4\)](#)

Экспорт добавленного вручную пользовательского образа ВМ (см. раздел 4.5)

Ручная настройка ОС на образе ВМ (см. раздел 4.6)

4.1. Установка и настройка VNC-сервера

Внимание! Для установки сервера WebVNC требуется доступ через интернет к сайту github.com.

- ▶ Чтобы установить и настроить сервер WebVNC,

выполните команды:

```
wget https://github.com/pgaskin/easy-novnc/releases/download/v1.1.0/easy-novnc_linux-64bit
chmod +x easy-novnc_linux-64bit
mv easy-novnc_linux-64bit /usr/local/bin/easy-novnc
```

Сервер WebVNC установлен и настроен.

4.2. Создание образа ВМ из ISO-файла

Внимание! Создание образа ВМ из ISO-файла поддерживается только для Windows 10, 11 и Windows Server версий 2016—2019.

В результате выполнения инструкции вы получите файл с расширением `.sandboximage`. Этот файл предназначенный для добавления образа ВМ в PT Email Security через веб-интерфейс. Размер файла не должен превышать 30 ГБ. Инструкцию по добавлению пользовательского образа в PT Email Security вы можете найти в Руководстве специалиста по безопасности.

- ▶ Чтобы создать образ ВМ из ISO-файла:

1. Подключитесь по протоколу SSH к одному из узлов PT Email Security с функцией поведенческого анализа:

```
ssh <Логин на узле>@<IP-адрес узла PT Email Security>
```

Пример:

```
ssh Administrator@192.0.2.25
```

2. Перейдите в каталог утилиты ImageBuilder:

```
cd /opt/ptms/sbin/
```

3. Создайте образ ВМ и установите на него ОС, выполнив команду:

```
sudo ./imagebuilder build-custom-image --boot-mode <Режим загрузки ОС> --expose-vnc <Порт подключения к VNC-серверу> --image-dir <Каталог для сохранения образа ВМ> --language <Язык ОС> --os-iso <Путь к ISO-файлу> --os-type windows --timezone <Часовой пояс ОС> --username-locale <Язык логина> --vm-memory <Объем памяти ВМ в MiB> --vm-name <Название временной ВМ>
```

Параметры команд утилиты ImageBuilder описаны в таблице ниже.

Пример:

```
sudo ./imagebuilder build-custom-image --boot-mode uefi --expose-vnc 5900 --image-dir /tmp/user_win7 --language en-US --os-iso /home/win7.iso --os-type windows --timezone Europe/Moscow --username-locale en-US --vm-memory 4096 --vm-name user_win7
```

Начнется установка и загрузка ОС.

4. Создайте еще одно подключение по протоколу SSH к тому же узлу PT Email Security.
5. Запустите VNC-сервер, выполнив команду:

```
easy-novnc --addr :<Порт веб-интерфейса VNC-сервера> --basic-ui --no-url-password --host <IP-адрес PT Email Security> --port <Порт подключения к VNC-серверу>
```

Пример:

```
easy-novnc --addr :8081 --basic-ui --no-url-password --host 192.0.2.25 --port 5900
```

6. Откройте браузер и в адресной строке введите:
`http://<IP-адрес PT Email Security>:<Порт веб-интерфейса VNC-сервера>`

Пример:

```
http://192.0.2.25:8081
```

7. На открывшейся странице нажмите кнопку **Connect**.

Запустится мастер установки Windows.

8. Следуйте указаниям мастера до завершения установки.

После перезагрузки откроется рабочий стол Windows.

Внимание! Если в ОС установлен антивирус или другое ПО для защиты информации отключите или удалите его.

9. Откройте интерфейс командной строки Windows от имени администратора и запустите настройку ОС, выполнив команду:

```
<Имя виртуального CD-привода>:\Invoke-PostInstall.cmd
```

Начнется настройка и перезагрузка ОС.

10. Если требуется, вручную настройте ОС на образе ВМ и [установите ПО \(см. раздел 4.6\)](#).

11. Экпортируйте файлы образа ВМ в файл с расширением `.sandboximage`, выполнив команду:

```
sudo ./imagebuilder export-image --image-dir <Каталог с образом ВМ> --output-name <Каталог для сохранения образа ВМ>/<Название образа ВМ>.sandboximage
```

Пример:

```
sudo ./imagebuilder export-image --image-dir /tmp/user_win7 --output-name /out/user_win7.sandboximage
```

Образ ВМ создан и экспортирован в файл для добавления в PT Email Security через веб-интерфейс.

Таблица 71. Параметры команд утилиты ImageBuilder

Параметр	Обязательный	Назначение	Пример
<code>--help <Команда></code>	—	Показать экранную справку утилиты и выйти	<code>--help build-custom-image</code>
Команда build-custom-image			
<code>--boot-mode <Режим загрузки ОС></code>	Да	Режим загрузки ОС: <code>bios</code> или <code>uefi</code>	<code>--boot-mode uefi</code>
<code>--expose-vnc <Порт></code>	Да	Порт для подключения к VNC-серверу (без пароля)	<code>--expose-vnc 5900</code>
<code>--hvm-template-dir <Каталог></code>	—	Каталог с шаблонами конфигурации Xen HVM	<code>--hvm-template-dir /etc/xen/hvm-templates</code>
<code>--image-dir <Каталог></code>	Да	Каталог для сохранения образа ВМ. Должен отличаться от <code>/opt/ptms/sandbox-images</code> . Может содержать латинские буквы, цифры и знак подчеркивания	<code>--image-dir tmp/user_win7</code>
<code>--language <Язык></code>	Да	Язык ОС. Один из языков, доступных в исходном образе	<code>--language en-US</code>
<code>--os-iso <Путь к ISO-файлу></code>	Да	Путь к ISO-файлу	<code>--os-iso /home/win7.iso</code>
<code>--os-type <Тип ОС></code>	Да	Тип ОС	<code>--os-type windows</code>
<code>--profile-cache-dir <Каталог></code>	—	Каталог для кэша профилей отладочных символов	<code>--profile-cache-dir /tmp/profiles</code>
<code>--sandbox-settings-file <Путь к файлу></code>	—	Путь к файлу <code>sandbox-settings.json</code> с дополнительными настройками ОС	<code>--sandbox-settings-file /home/sandbox-settings.json</code>
<code>--timezone <Часовой пояс></code>	Да	Часовой пояс ОС в формате IANA	<code>--timezone Europe/Moscow</code>
<code>--usb-drive <Путь к файлу></code>	—	Путь к файлу QCOW2-образа USB-накопителя	<code>--usb-drive /tmp/usb_data.qcow2</code>

Параметр	Обязательный	Назначение	Пример
<code>--username-locale <Язык></code>	Да	Язык логина пользователя ОС	<code>--username-locale en-US</code>
<code>--vm-memory <Объем в MiB></code>	Да	Объем памяти ОЗУ временной VM в MiB (не менее 2048)	<code>--vm-memory 4096</code>
<code>--vm-name <Имя></code>	Да	Название временной VM	<code>--vm-name user_win7</code>
<code>--windows-assets-dir <Каталог></code>	—	Каталог с компонентами PT Email Security для ПА в Windows	<code>--windows-assets-dir /opt/win-utils</code>
<code>--windows-auto-install-cfg-dir <Каталог></code>	—	Каталог с шаблонами автоматической установки Windows	<code>--windows-auto-install-cfg-dir /opt/win-autoinstall</code>
<code>--windows-dll-hooks-dir <Каталог></code>	—	Каталог с DLL-хуками для Windows	<code>--windows-dll-hooks-dir /opt/win-dll-hooks</code>

Команда <code>export-image</code>			
<code>--output-name <Путь к файлу></code>	Да	Существующий каталог и название файла с расширением <code>.sandboximage</code> для сохранения образа VM	<code>--output-name /out/user_win7.sandboximage</code>
<code>--image-dir <Каталог></code>	Да	Каталог с образом VM для экспорта	<code>--image-dir /tmp/user_win7</code>

4.3. Создание образа VM из образа диска в формате QCOW2

Внимание! Создание образа VM из образа диска в формате QCOW2 поддерживается только для Windows 10, 11.

Примечание. Вы можете конвертировать образ диска в формат QCOW2 с помощью сторонних утилит. Например, из формата RAW с помощью утилиты `qemu-img` командой `qemu-img convert -c -O qcow2 -o cluster_size=64K image.raw image.qcow2`.

В результате выполнения инструкции вы получите файл с расширением `.sandboximage`. Этот файл предназначенный для добавления образа VM в PT Email Security через веб-интерфейс. Размер файла не должен превышать 30 ГБ. Инструкцию по добавлению пользовательского образа в PT Email Security вы можете найти в Руководстве специалиста по безопасности.

► Чтобы создать образ VM Windows из образа диска в формате QCOW2:

1. Подключитесь по протоколу SSH к одному из узлов PT Email Security с функцией поведенческого анализа:

```
ssh <Логин на узле>@<IP-адрес узла PT Email Security>
```

Пример:

```
ssh Administrator@192.0.2.25
```

2. Перейдите в каталог утилиты ImageBuilder:

```
cd /opt/ptms/sbin/
```

3. Импортируйте образ VM из образа диска в формате QCOW2, выполнив команду:

```
sudo ./imagebuilder import-custom-image --disk-drive <Путь к образу в формате QCOW2> --  
expose-vnc <Порт подключения к VNC-серверу> --image-dir <Каталог для сохранения образа> --  
language <Язык ОС> --os-type windows --timezone <Часовой пояс ОС> --username-locale <Язык  
логина> --vm-memory <Объем памяти VM в MiB> --vm-name <Название временной VM>
```

Параметры команд утилиты ImageBuilder описаны в таблице ниже.

Пример:

```
sudo ./imagebuilder import-custom-image --disk-drive /home/win7.qcow2 --expose-vnc 5900 --  
image-dir /tmp/user_win7 --language en-US --os-type windows --timezone Europe/Moscow --  
username-locale en-US --vm-memory 4096 --vm-name user_win7
```

Начнется импорт образа VM и загрузка ОС.

4. Создайте еще одно подключение по протоколу SSH к тому же узлу PT Email Security.
5. Запустите VNC-сервер, выполнив команду:

```
easy-novnc --addr :<Порт веб-интерфейса VNC-сервера> --basic-ui --no-url-password --host  
<IP-адрес PT Email Security> --port <Порт подключения к VNC-серверу>
```

Пример:

```
easy-novnc --addr :8081 --basic-ui --no-url-password --host 192.0.2.25 --port 5900
```

6. Откройте браузер и в адресной строке введите:

```
http://<IP-адрес PT Email Security>:<Порт веб-интерфейса VNC-сервера>
```

Пример:

```
http://192.0.2.25:8081
```

7. На открывшейся странице нажмите кнопку **Connect**.

Откроется рабочий стол Windows.

Внимание! Если в ОС установлен антивирус или другое ПО для защиты информации отключите или удалите его.

8. Откройте интерфейс командной строки Windows от имени администратора и запустите настройку ОС, выполнив команду:

```
<Имя виртуального CD-привода>:\Invoke-PostInstall.cmd
```

Начнется настройка и перезагрузка ОС.

9. Если требуется, вручную настройте ОС на образе VM и [установите ПО](#) (см. раздел 4.6).

10. Экпортируйте файлы образа VM в файл с расширением `.sandboximage`, выполнив команду:

```
sudo ./imagebuilder export-image --image-dir <Каталог с образом VM> --output-name <Каталог для сохранения образа VM>/<Название образа VM>.sandboximage
```

Пример:

```
sudo ./imagebuilder export-image --image-dir /tmp/user_win7 --output-name /out/user_win7.sandboximage
```

Образ VM создан и экспортирован в файл для добавления в PT Email Security через веб-интерфейс.

Таблица 72. Параметры команд утилиты ImageBuilder

Параметр	Обязательный	Назначение	Пример
<code>--help <Команда></code>	—	Показать экранную справку утилиты и выйти	<code>--help import-custom-image</code>
Команда <code>import-custom-image</code>			
<code>--disk-drive <Путь к образу></code>	Да	Путь к образу в формате QCOW	<code>--disk-drive /home/win7.qcow2</code>
<code>--expose-vnc <Порт></code>	Да	Порт для подключения к VNC-серверу (без пароля)	<code>--expose-vnc 5900</code>
<code>--hvm-template-dir <Каталог></code>	—	Каталог с шаблонами конфигурации Xen HVM	<code>--hvm-template-dir /etc/xen/hvm-templates</code>
<code>--image-dir <Каталог></code>	Да	Каталог для сохранения образа VM. Должен отличаться от <code>/opt/ptms/sandbox-images</code> . Может содержать латинские буквы, цифры и знак подчеркивания	<code>--image-dir tmp/user_win7</code>
<code>--language <Язык></code>	Да	Язык ОС. Один из языков, доступных в исходном образе	<code>--language en-US</code>
<code>--os-type <Тип ОС></code>	Да	Тип ОС	<code>--os-type windows</code>
<code>--profile-cache-dir <Каталог></code>	—	Каталог для кэша профилей отладочных символов	<code>--profile-cache-dir /tmp/profiles</code>

Параметр	Обязательный	Назначение	Пример
--sandbox-settings-file <Путь к файлу>	—	Путь к файлу sandbox-settings.json с дополнительными настройками ОС	--sandbox-settings-file /home/sandbox-settings.json
--timezone <Часовой пояс>	Да	Часовой пояс ОС в формате IANA	--timezone Europe/Moscow
--usb-drive <Путь к файлу>	—	Путь к файлу QCOW2-образа USB-накопителя	--usb-drive /tmp/usb_data.qcow2
--username-locale <Язык>	Да	Язык логина пользователя ОС	--username-locale en-US
--vm-memory <Объем в MiB>	Да	Объем памяти ОЗУ временной ВМ в MiB (не менее 2048)	--vm-memory 4096
--vm-name <Имя>	Да	Название временной ВМ	--vm-name user_win7
--windows-assets-dir <Каталог>	—	Каталог с компонентами PT Email Security для ПА в Windows	--windows-assets-dir /opt/win-utils
--windows-auto-install-cfg-dir <Каталог>	—	Каталог с шаблонами автоматической установки Windows	--windows-auto-install-cfg-dir /opt/win-autoinstall
--windows-dll-hooks-dir <Каталог>	—	Каталог с DLL-хуками для Windows	--windows-dll-hooks-dir /opt/win-dll-hooks
Команда export-image			
--output-name <Путь к файлу>	Да	Существующий каталог и название файла с расширением .sandboximage для сохранения образа ВМ	--output-name /out/user_win7.sandboximage
--image-dir <Каталог>	Да	Каталог с образом ВМ для экспорта	--image-dir /tmp/user_win7

4.4. Копирование добавленного ранее образа ВМ

Вы можете скопировать и настроить образ ВМ, который уже добавлен в PT Email Security.

В результате выполнения инструкции вы получите файл с расширением `.sandboximage`. Этот файл предназначенный для добавления образа ВМ в PT Email Security через веб-интерфейс. Размер файла не должен превышать 30 ГБ. Инструкцию по добавлению пользовательского образа в PT Email Security вы можете найти в Руководстве специалиста по безопасности.

► Чтобы скопировать образ ВМ из образа, добавленного ранее в PT Email Security:

1. Подключитесь по протоколу SSH к одному из узлов PT Email Security с функцией поведенческого анализа:

```
ssh <Логин на узле>@<IP-адрес узла PT Email Security>
```

Пример:

```
ssh Administrator@192.0.2.25
```

2. Перейдите в каталог утилиты ImageBuilder:

```
cd /opt/ptms/sbin/
```

3. Скопируйте образ ВМ, выполнив команду:

```
sudo ./imagebuilder customize-image --customized-image-name <Имя нового образа ВМ> --expose-vnc <Порт подключения к VNC-серверу> --image-name <Имя исходного образа ВМ> --installed-images-dir <Каталог исходного образа ВМ> --tmp-dir <Каталог для временных файлов> --vm-memory <Объем памяти ВМ в MiB> --vm-name <Название временной ВМ>
```

Параметры команд утилиты ImageBuilder описаны в таблице ниже.

Пример:

```
sudo ./imagebuilder customize-image --customized-image-name user_win7-sp1-x64 --expose-vnc 5900 --image-name win7-sp1-x64 --installed-images-dir /opt/ptms/sandbox-images --tmp-dir /tmp/user_win7 --vm-memory 4096 --vm-name user_win7
```

Образ ВМ будет скопирован в указанный каталог для временных файлов.

4. Создайте еще одно подключение по протоколу SSH к тому же узлу PT Email Security.
5. Запустите VNC-сервер, выполнив команду:

```
easy-novnc --addr <Порт веб-интерфейса VNC-сервера> --basic-ui --no-url-password --host <IP-адрес PT Email Security> --port <Порт подключения к VNC-серверу>
```

Пример:

```
easy-novnc --addr :8081 --basic-ui --no-url-password --host 192.0.2.25 --port 5900
```

6. Откройте браузер и в адресной строке введите:

```
http://<IP-адрес PT Email Security>:<Порт веб-интерфейса VNC-сервера>
```

Пример:

```
http://192.0.2.25:8081
```

7. На открывшейся странице нажмите кнопку **Connect**.

Откроется рабочий стол Windows.

8. Вручную настройте ОС на образе VM и [установите ПО \(см. раздел 4.6\)](#).

9. Экпортируйте файлы образа VM в файл с расширением `.sandboximage`, выполнив команду:

```
sudo ./imagebuilder export-image --image-dir <Каталог с образом VM> --output-name <Каталог для сохранения образа VM>/<Название образа VM>.sandboximage
```

Пример:

```
sudo ./imagebuilder export-image --image-dir /tmp/user_win7 --output-name /out/user_win7.sandboximage
```

Образ VM скопирован и экспортирован в файл для добавления в PT Email Security через веб-интерфейс.

Таблица 73. Параметры команд утилиты ImageBuilder

Параметр	Обязательный	Назначение	Пример
<code>--help <Команда></code>	—	Показать экранную справку утилиты и выйти	<code>--help customize-image</code>
Команда <code>customize-image</code>			
<code>--customized-image-name <Имя></code>	Да	Имя нового образа VM	<code>--customized-image-name vm-custom</code>
<code>--expose-vnc <Порт></code>	Да	Порт для подключения к VNC-серверу (без пароля)	<code>--expose-vnc 5900</code>
<code>--image-name <Имя></code>	Да	Имя исходного образа VM	<code>--image-name debian-base</code>
<code>--installed-images-dir <Каталог></code>	Да	Каталог с установленными в PT Email Security образами VM <code>/opt/ptms/sandbox-images</code>	<code>--installed-images-dir /opt/ptms/sandbox-images</code>
<code>--linux-assets-dir <Каталог></code>	—	Каталог с компонентами PT Email Security для ПА в ОС семейства Linux	<code>--linux-assets-dir /opt/linux-utils</code>
<code>--profile-cache-dir <Каталог></code>	—	Каталог для кэша профилей отладочных символов	<code>--profile-cache-dir /tmp/profiles</code>
<code>--sandbox-settings-file <Путь к файлу></code>	—	Путь к файлу <code>sandbox-settings.json</code> с дополнительными настройками ОС	<code>--sandbox-settings-file /home/sandbox-settings.json</code>

Параметр	Обязательный	Назначение	Пример
<code>--tmp-dir <Каталог></code>	Да	Временный каталог для файлов VM	<code>--tmp-dir /tmp/vmfiles</code>
<code>--vm-memory <Объем в MiB></code>	Да	Объем памяти ОЗУ временной VM в MiB (не менее 2048)	<code>--vm-memory 4096</code>
<code>--vm-name <Имя></code>	Да	Название временной VM	<code>--vm-name user_win7</code>
<code>--windows-assets-dir <Каталог></code>	—	Каталог с компонентами PT Email Security для ПА в Windows	<code>--windows-assets-dir /opt/win-utils</code>
<code>--windows-dll-hooks-dir <Каталог></code>	—	Каталог с DLL-хуками для Windows	<code>--windows-dll-hooks-dir /opt/win-dll-hooks</code>
Команда export-image			
<code>--output-name <Путь к файлу></code>	Да	Существующий каталог и название файла с расширением <code>.sandboximage</code> для сохранения образа VM	<code>--output-name /out/user_win7.sandboximage</code>
<code>--image-dir <Каталог></code>	Да	Каталог с образом VM для экспорта	<code>--image-dir /tmp/user_win7</code>

4.5. Экспорт добавленного вручную пользовательского образа VM

Если вы добавляли в PT Email Security пользовательские образы VM, и если эти образы были вручную скопированы на узлы с функцией поведенческого анализа, рекомендуется заново добавить такие образы в PT Email Security через веб-интерфейс. Это обеспечивает автоматическое управление образами VM на всех узлах с функцией поведенческого анализа. Для этого вам необходимо:

1. Экспортировать добавленный вручную образ VM из PT Email Security в файл с расширением `.sandboximage`. Размер получившегося файла не должен превышать 30 ГБ.
2. Скачать полученный файл с образом VM на ваш компьютер.
3. Добавить образ VM из полученного файла в PT Email Security через веб-интерфейс.

Примечание. Инструкции по добавлению пользовательского образа VM в PT Email Security и настройке параметров проверки объектов вы можете найти в Руководстве специалиста по безопасности.

4. В параметрах проверки объектов выбрать образ ВМ, добавленный через веб-интерфейс, вместо образа ВМ, добавленного вручную.
5. Удалить добавленный вручную образ ВМ из PT Email Security.

► Чтобы экспортировать добавленный вручную пользовательский образ ВМ из PT Email Security:

1. Подключитесь по протоколу SSH к одному из узлов PT Email Security с функцией поведенческого анализа:

```
ssh <Логин на узле>@<IP-адрес узла PT Email Security>
```

Пример:

```
ssh Administrator@192.0.2.25
```

2. Перейдите в каталог утилиты ImageBuilder:

```
cd /opt/ptms/sbin/
```

3. Экспортируйте добавленный вручную образ ВМ в файл с расширением `.sandboximage`, выполнив команду:

```
sudo ./imagebuilder export-image --output-name <Каталог для сохранения образа ВМ>/  
<Название образа ВМ>.sandboximage --image-dir /opt/ptms/sandbox-images/custom_<Каталог с  
файлами образа ВМ>
```

Параметры команд утилиты ImageBuilder описаны в таблице ниже.

Пример:

```
sudo ./imagebuilder export-image --output-name /out/user_win7.sandboximage --image-dir /  
opt/ptms/sandbox-images/custom_win7
```

Образ ВМ экспортирован в файл для добавления в PT Email Security через веб-интерфейс.

► Чтобы скачать файл с образом ВМ на ваш компьютер,

выполните команду:

```
scp <Логин на узле>@<IP-адрес узла>:<Каталог для сохранения образа ВМ>/<Название образа  
ВМ>.sandboximage <Локальный каталог>/<Название образа ВМ>.sandboximage
```

Пример:

```
scp Administrator@192.0.3.22:/out/user_win7.sandboximage /tmp/user_win7.sandboximage
```

► Чтобы удалить добавленный вручную пользовательский образ ВМ из PT Email Security,

последовательно для каждого узла PT Email Security с функцией поведенческого анализа выполните команду:

```
ssh <Логин на узле>@<IP-адрес узла PT Email Security> "rm -rf /opt/ptms/sandbox-images/  
<Каталог с файлами образа ВМ>"
```

Образы ВМ хранятся в каталоге `/opt/ptms/sandbox-images`. Имя каталога с файлами добавленного вручную образа ВМ начинается с префикса `custom_`.

Пример:

```
ssh Administrator@192.0.3.11 "rm -rf /opt/ptms/sandbox-images/custom_win7"
```

Пользовательский образ VM удален из PT Email Security.

Таблица 74. Параметры команд утилиты ImageBuilder

Параметр	Обязательный	Назначение	Пример
<code>--help <Команда></code>	—	Показать экранную справку утилиты и выйти	<code>--help export-image</code>
Команда export-image			
<code>--output-name <Путь к файлу></code>	Да	Существующий каталог и название файла с расширением <code>.sandboximage</code> для сохранения образа VM	<code>--output-name /out/user_win7.sandboximage</code>
<code>--image-dir <Каталог></code>	Да	Каталог с образом VM для экспорта	<code>--image-dir /tmp/user_win7</code>

4.6. Ручная настройка ОС на образе VM

Перед ручной настройкой ОС необходимо создать или скопировать образ VM. При ручной настройке ОС вы можете, например, установить ПО, изменить язык интерфейса и активировать Windows.

Внимание! В ОС на образах VM не рекомендуется устанавливать антивирусы или другое ПО для защиты информации. Это может привести к неработоспособности образа или большому числу ложных срабатываний при поведенческом анализе файлов. Если такое ПО уже установлено в ОС, рекомендуется отключить или удалить его.

При настройке ОС на образе VM предоставляется доступ к внешним ресурсам через прокси-сервер PT Email Security.

► Чтобы вручную настроить ОС на образе VM:

1. Если вы создали образ VM из ISO-файла или из образа диска в формате QCOW2, запустите настройку образа VM, выполнив команду:

```
sudo ./imagebuilder run-image --expose-vnc <Порт подключения к VNC-серверу> --image-dir <Каталог с образом VM> --vm-memory <Объем памяти VM в MiB> --vm-name <Название временной VM>
```

Параметры команд утилиты ImageBuilder описаны в таблице ниже.

Пример:

```
sudo ./imagebuilder run-image --expose-vnc 5900 --image-dir /tmp/user_win7 --vm-memory 4096 --vm-name user_win7
```

Начнется загрузка ОС.

2. Через открытый в браузере проводник Windows настройте ОС и установите ПО (см. инструкцию ниже).
3. Нажмите клавишу Enter.

Настройка ОС на образе ВМ завершена.

Таблица 75. Параметры команд утилиты ImageBuilder

Параметр	Обязательный	Назначение	Пример
--help <Команда>	—	Показать экранную справку утилиты и выйти	--help run-image
Команда run-image			
--expose-vnc <Порт>	Да	Порт для подключения к VNC-серверу (без пароля)	--expose-vnc 5900
--image-dir <Каталог>	Да	Каталог для сохранения образа ВМ. Должен отличаться от /opt/ptms/sandbox-images. Может содержать латинские буквы, цифры и знак подчеркивания	--image-dir tmp/user_win7
--linux-assets-dir <Каталог>	—	Каталог с компонентами PT Email Security для ПА в ОС семейства Linux	--linux-assets-dir /opt/linux-utils
--profile-cache-dir <Каталог>	—	Каталог для кэша профилей отладочных символов	--profile-cache-dir /tmp/profiles
--sandbox-settings-file <Путь к файлу>	—	Путь к файлу sandbox-settings.json с дополнительными настройками ОС	--sandbox-settings-file /home/sandbox-settings.json
--vm-memory <Объем в MiB>	Да	Объем памяти ОЗУ временной ВМ в MiB (не менее 2048)	--vm-memory 4096
--vm-name <Имя>	Да	Название временной ВМ	--vm-name user_win7

Параметр	Обязательный	Назначение	Пример
<code>--windows-assets-dir <Каталог></code>	—	Каталог с компонентами PT Email Security для ПА в Windows	<code>--windows-assets-dir /opt/win-utils</code>
<code>--windows-dll-hooks-dir <Каталог></code>	—	Каталог с DLL-хуками для Windows	<code>--windows-dll-hooks-dir /opt/win-dll-hooks</code>

Установка ПО с помощью менеджера пакетов Chocolatey

- ▶ Чтобы установить ПО на образ VM с помощью менеджера пакетов Chocolatey:
 1. Через открытый в браузере проводник Windows откройте интерфейс командной строки Windows от имени администратора.
 2. Если менеджер пакетов Chocolatey не установлен, установите его, выполнив команду:
`C:\guest-utils\Configure-Sandbox.cmd Install-Chocolatey`
 3. Установите ПО, выполнив соответствующие команды, например:


```
choco install visioviewer2016 --version=16.0 -y
choco install vlc --version=3.0.8 -y
choco install irfanview --version=4.54 -y
choco install windjview --version=2.1 -y --ignore-checksum
choco install paint.net --version=4.2.9 -y
choco install vcredist-all -y
```

ПО установлено.

Установка ПО с локального веб-сервера

- ▶ Чтобы установить ПО на образ VM с локального веб-сервера:
 1. Используя терминальный клиент, перейдите на узле с PT Email Security в каталог с ПО для установки и выполните команду:
`ip netns exec <Имя VM в Xen> python3 -m http.server <Порт веб-сервера>`
 2. Через открытый в браузере проводник Windows откройте интерфейс командной строки Windows от имени администратора.
 3. Определите IP-адрес шлюза, выполнив команду:
`ipconfig`
 IP-адрес шлюза указан в поле Default Gateway.

4. На узле с PT Email Security запустите браузер и перейдите по ссылке:

`http://<IP-адрес шлюза>:<Порт веб-сервера>`

5. Скачайте и установите необходимое ПО.

ПО установлено.

Установка ПО с виртуального CD-привода

Если в образе VM есть виртуальный CD-привод, вы можете установить ПО из смонтированного на него ISO-файла.

- ▶ Чтобы установить ПО с виртуального CD-привода:

1. Используя терминальный клиент, узнайте имя виртуального CD-привода:

```
sudo xl qemu-monitor-command <Название временной VM> "info block"
```

Пример:

```
sudo xl qemu-monitor-command custom_win7 "info block"
```

2. Смонтируйте ISO-файл с ПО на виртуальный CD-привод:

```
sudo xl qemu-monitor-command <Название временной VM> "change <Имя виртуального CD-привода>  
<Абсолютный путь к ISO-файлу>"
```

Пример:

```
sudo xl qemu-monitor-command custom_win7 "change ide1-cd0 /home/soft.iso"
```

Установите необходимое ПО с ISO-файла.

ПО установлено.

5. О технической поддержке

Гарантийная поддержка доступна для всех владельцев действующих лицензий на PT Email Security в течение периода предоставления обновлений и включает в себя следующий набор услуг.

Предоставление доступа к обновленным версиям продукта

Обновления продукта выпускаются в порядке и в сроки, определяемые Positive Technologies. Positive Technologies предоставляет обновленные версии продукта в течение оплаченного периода получения обновлений, указанного в бланке лицензии приобретенного продукта Positive Technologies.

Positive Technologies не производит установку обновлений продукта в рамках гарантийной поддержки и не несет ответственности за инциденты, возникшие в связи с некорректной или несвоевременной установкой обновлений продукта.

Восстановление работоспособности продукта

Специалист Positive Technologies проводит диагностику заявленного сбоя и предоставляет рекомендации для восстановления работоспособности продукта. Восстановление работоспособности может заключаться в выдаче рекомендаций по установке продукта заново с потенциальной потерей накопленных данных либо в восстановлении версии продукта из доступной резервной копии (резервное копирование должно быть настроено заблаговременно). Positive Technologies не несет ответственности за потерю данных в случае неверно настроенного резервного копирования.

Примечание. Помощь оказывается при условии, что конечным пользователем продукта соблюдены все аппаратные, программные и иные требования и ограничения, описанные в документации к продукту.

Устранение ошибок и дефектов в работе продукта в рамках выпуска обновленных версий

Если в результате диагностики обнаружен дефект или ошибка в работе продукта, Positive Technologies обязуется включить исправление в ближайшие возможные обновления продукта (с учетом релизного цикла продукта, приоритета дефекта или ошибки, сложности требуемых изменений, а также экономической целесообразности исправления). Сроки выпуска обновлений продукта остаются на усмотрение Positive Technologies.

Рассмотрение предложений по доработке продукта

При обращении с предложением по доработке продукта необходимо подробно описать цель такой доработки. Вы можете поделиться рекомендациями по улучшению продукта и оптимизации его функциональности. Positive Technologies обязуется рассмотреть все предложения, однако не принимает на себя обязательств по реализации каких-либо

доработок. Если Positive Technologies принимает решение о доработке продукта, то способы ее реализации остаются на усмотрение Positive Technologies. Заявки принимаются [на портале технической поддержки](#).

Портал технической поддержки

[На портале технической поддержки](#) вы можете круглосуточно создавать и обновлять заявки и читать новости продуктов.

Для получения доступа к portalу технической поддержки нужно создать учетную запись, используя адрес электронной почты в официальном домене вашей организации. Вы можете указать другие адреса электронной почты в качестве дополнительных. Добавьте в профиль название вашей организации и контактный телефон — так нам будет проще с вами связаться.

Поддержка на портале предоставляется на русском и английском языках.

Условия предоставления гарантийной поддержки

Для получения гарантийной поддержки необходимо оставить заявку [на портале технической поддержки](#) и предоставить следующие данные:

- номер лицензии на использование продукта;
- файлы журналов и наборы диагностических данных, которые требуются для анализа;
- снимки экрана.

Positive Technologies не берет на себя обязательств по оказанию услуг гарантийной поддержки в случае вашего отказа предоставить запрашиваемую информацию или отказа от внедрения предоставленных рекомендаций.

Если заказчик не предоставляет необходимую информацию по прошествии 20 календарных дней с момента ее запроса, специалист технической поддержки имеет право закрыть заявку. Оказание услуг может быть возобновлено по вашей инициативе при условии предоставления запрошенной ранее информации.

Услуги по гарантийной поддержке продукта не включают в себя услуги по переустановке продукта, решение проблем с операционной системой, инфраструктурой заказчика или сторонним программным обеспечением.

Заявки могут направлять уполномоченные сотрудники заказчика, владеющего продуктом на законном основании (включая наличие действующей лицензии). Специалисты заказчика должны иметь достаточно знаний и навыков для сбора и предоставления диагностической информации, необходимой для решения заявленной проблемы.

Услуги по гарантийной поддержке оказываются в отношении поддерживаемых версий продукта. Информация о поддерживаемых версиях содержится в «Политике поддержки версий программного обеспечения» и (или) иных информационных материалах, размещенных на официальном веб-сайте Positive Technologies.

Время реакции и приоритизация заявок

При получении заявки ей присваивается регистрационный номер, специалист службы технической поддержки классифицирует ее (присваивает тип и уровень значимости) и выполняет дальнейшие шаги по ее обработке.

Время реакции рассчитывается с момента получения заявки до первичного ответа специалиста технической поддержки с уведомлением о взятии заявки в работу. Время реакции зависит от уровня значимости заявки. Специалист службы технической поддержки оставляет за собой право переопределить уровень значимости в соответствии с приведенными ниже критериями. Указанные сроки являются целевыми, но возможны отклонения от них по объективным причинам.

Таблица 76. Время реакции на заявку

Уровень значимости заявки	Критерии значимости заявки	Время реакции на заявку
Критический	Аварийные сбои, приводящие к невозможности штатной работы продукта (исключая первоначальную установку) либо оказывающие критически значимое влияние на бизнес заказчика	До 4 часов
Высокий	Сбои, проявляющиеся в любых условиях эксплуатации продукта и оказывающие значительное влияние на бизнес заказчика	До 8 часов
Средний	Сбои, проявляющиеся в специфических условиях эксплуатации продукта либо не оказывающие значительного влияния на бизнес заказчика	До 8 часов
Низкий	Вопросы информационного характера либо сбои, не влияющие на эксплуатацию продукта	До 8 часов

Указанные часы относятся к рабочему времени (рабочие дни с 9:00 до 18:00 UTC+3) специалистов технической поддержки. Под рабочим днем понимается любой день за исключением субботы, воскресенья и дней, являющихся официальными нерабочими днями в Российской Федерации.

Обработка и закрытие заявок

По мере рассмотрения заявки и выполнения необходимых действий специалист службы поддержки сообщает вам:

- о ходе диагностики по заявленной проблеме и ее результатах;
- планах выпуска обновленной версии продукта (если требуется для устранения проблемы).

Если по итогам обработки заявки необходимо внести изменения в продукт, Positive Technologies включает работы по исправлению в ближайшее возможное плановое обновление продукта (с учетом релизного цикла продукта, приоритета дефекта или ошибки, сложности требуемых изменений, а также экономической целесообразности исправления). Сроки выпуска обновлений продукта остаются на усмотрение Positive Technologies.

Специалист закрывает заявку, если:

- предоставлены решение или возможность обойти проблему, не влияющие на критически важную функциональность продукта (по усмотрению Positive Technologies);
- диагностирован дефект продукта, собрана техническая информация о дефекте и условиях его воспроизведения, исправление дефекта запланировано к выходу в рамках планового обновления продукта;
- заявленная проблема вызвана программным обеспечением или оборудованием сторонних производителей, на которые не распространяются обязательства Positive Technologies;
- заявленная проблема классифицирована специалистами Positive Technologies как неподдерживаемая.

Примечание. Если продукт приобретался вместе с аппаратной платформой в виде программно-аппаратного комплекса (ПАК), решение заявок, связанных с ограничением или отсутствием работоспособности аппаратных компонентов, происходит согласно условиям и срокам, указанным в гарантийных обязательствах (гарантийных талонах) на такие аппаратные компоненты.



Positive Technologies — один из лидеров в области результативной кибербезопасности. Компания является ведущим разработчиком продуктов, решений и сервисов, позволяющих выявлять и предотвращать кибератаки до того, как они причинят неприемлемый ущерб бизнесу и целым отраслям экономики. Positive Technologies — первая и единственная компания из сферы кибербезопасности на Московской бирже (MOEX: POSI). Количество акционеров превышает 220 тысяч.