positive technologies

PT Industrial Security Incident Manager

White paper: реализация требований стандарта ISA/IEC 62443-3-3 с помощью продукта PT ISIM

Оглавление

1. О чем этот документ и для кого он предназначен 3
2. Расширенный обзор: назначение и структура раздела 3-3 стандарта ISA/IEC 62443 4
3. Общие сведения о PT ISIM, его назначении и возможностях 5
4. Матрица покрытия: реализация требований ISA/IEC 62443-3-3 средствами PT ISIM 6
5. Заключение 14

1. О чем этот документ и для кого он предназначен

Настоящий документ (white paper) представляет собой аналитический обзор и практическое руководство по реализации системных требований кибербезопасности, описанных в международном стандарте ISA/IEC 62443-3-3, с использованием комплексной системы обеспечения киберустойчивости OT-инфраструктур PT Industrial Security Incident Manager (PT ISIM) компании Positive Technologies.

Целевая аудитория документа

- Директора по информационной безопасности (CISO) и руководители профильных подразделений промышленных предприятий.
- Специалисты центров мониторинга информационной безопасности (SOC), аналитики и инженеры по ИБ.
- Архитекторы АСУ ТП и специалисты по сетевой инфраструктуре (OT-, ICS-инженеры).
- Интеграторы систем промышленной автоматизации и ИТ-решений.
- Лица, принимающие решения, ответственные за обеспечение непрерывности технологических процессов и защиту критической информационной инфраструктуры (КИИ).

2. Расширенный обзор: назначение и структура раздела 3-3 стандарта ISA/IEC 62443

Стандарт **ISA/IEC 62443** является ключевым мировым сводом правил и рекомендаций по обеспечению кибербезопасности систем промышленной автоматизации и управления (IACS / АСУ ТП).

Часть **ISA/IEC 62443-3-3 («Системные требования безопасности и уровни безопасности»)** занимает центральное место в техническом блоке стандарта. Ее основное назначение — определение конкретных технических требований к системе управления, которые необходимы для достижения заданных целевых уровней безопасности (Security Levels — SL).

Общее описание структуры

Документ базируется на семи основополагающих требованиях (foundational requirements, FR), которые формируют фундамент киберзащиты промышленной среды:

1. **FR 1: контроль идентификации и аутентификации (IAC)** — подтверждение личности пользователей, устройств и процессов.
2. **FR 2: контроль использования (UC)** — применение политик авторизации, контроль сессий и мобильного кода, ведение журналов аудита.
3. **FR 3: целостность системы (SI)** — защита информации и каналов связи от несанкционированных изменений, защита от вредоносного кода.
4. **FR 4: конфиденциальность данных (DC)** — предотвращение утечек данных в состоянии покоя или при передаче.
5. **FR 5: ограничение потоков данных (RDF)** — сегментация сети, изоляция зон и управление сетевыми границами.
6. **FR 6: своевременное реагирование на события (TRE)** — мониторинг, доступ к журналам аудита и выявление нарушений.
7. **FR 7: доступность ресурсов (RA)** — защита от DoS-атак, управление конфигурациями и резервное копирование.

Каждое фундаментальное требование разбивается на системные требования (system requirements, SR) и дополнительные усиления требований (requirement enhancements, RE), применимость которых зависит от того, какой уровень безопасности (от SL-1 до SL-4) необходим для конкретной производственной зоны.

3. Общие сведения о PT ISIM, его назначении и возможностях

PT Industrial Security Incident Manager (PT ISIM) — это передовая система обеспечения киберустойчивости промышленных инфраструктур, разрабатываемая компанией Positive Technologies.

Назначение

Продукт предназначен для непрерывного и глубокого анализа трафика технологических сетей, инвентаризации активов АСУ ТП, а также превентивного поиска угроз (threat hunting). PT ISIM позволяет своевременно выявлять кибератаки на ранних стадиях, обнаруживать ошибки конфигурации, несанкционированные действия персонала или подрядчиков без малейшего вмешательства в производственный процесс.

Ключевые возможности и особенности:

- **Пассивный мониторинг и полная безопасность для АСУ ТП.** PT ISIM получает копию трафика через SPAN-порты или TAP-устройства, работая в пассивном режиме, что исключает возможность негативного влияния на технологический процесс.
- **Глубокая инвентаризация и сетевая видимость.** Автоматическое обнаружение оборудования, построение карты сети, профилирование сетевых взаимодействий. Система собирает данные как безагентным методом, так и с помощью агентов (PT ISIM Endpoint Agent) и активного сканирования.
- **Обнаружение угроз (PT ISTI).** Использование уникальной постоянно обновляемой базы индикаторов промышленных угроз — PT Industrial Security Threat Indicators — позволяет выявлять эксплуатацию уязвимостей, активность вредоносного ПО (включая встроенный антивирусный модуль), аномалии и опасные команды, передаваемые по промышленным протоколам (поддерживаются десятки протоколов, включая специфические).
- **Централизованное управление и масштабирование.** Архитектура решения, включающая сенсоры (PT ISIM View Sensor), коллекторы (PT ISIM Collector), программные агенты для конечных точек (PT ISIM Endpoint Agent), центр управления (PT ISIM Overview Center), обеспечивает построение распределенных центров мониторинга технологических сетей (Industrial SOC) в компаниях любых масштабов.

4. Матрица покрытия: реализация требований ISA/IEC 62443-3-3 средствами PT ISIM

Ниже представлено сопоставление требований стандарта и функциональных возможностей PT ISIM (в таблицу включены только те требования, которые покрываются функциональными возможностями компонентов продукта):

Идентификатор требования	Название требования 62443 3-3	Содержание требования 62443 3-3	Покрытие требований функциональностью PT ISIM	Компонент PT ISIM
SR 1.2	Идентификация и аутентификация программных процессов и устройств	Система управления должна предоставлять возможность идентифицировать и аутентифицировать все программные процессы и устройства	PT ISIM позволяет идентифицировать устройства, программное обеспечение и процессы компонентов систем управления за счет инвентаризации сетевых узлов, анализа сетевого трафика и сканирования сети	PT ISIM View Sensor, PT ISIM Collector, PT ISIM Endpoint Agent
SR 1.2 (1)	Уникальная идентификация и аутентификация	Система управления должна предоставлять возможность уникально идентифицировать и аутентифицировать все программные процессы и устройства	PT ISIM позволяет идентифицировать устройства, программное обеспечение и процессы компонентов систем управления за счет инвентаризации сетевых узлов, анализа сетевого трафика и сканирования сети	PT ISIM View Sensor, PT ISIM Collector, PT ISIM Endpoint Agent
SR 1.13	Доступ через недоверенные сети	Система управления должна предоставлять возможность мониторить и контролировать все методы доступа к системе управления через недоверенные сети	PT ISIM позволяет реализовать мониторинг и контроль сетевого доступа, полученного через недоверенные сети, посредством анализа сетевого трафика систем управления, а также мониторинга событий и попыток доступа на конечных узлах систем управления	PT ISIM View Sensor, PT ISIM Collector, PT ISIM Endpoint Agent
SR 2.2	Контроль использования беспроводной связи	Система управления должна предоставлять возможность авторизовать и мониторить устройства, а также применять к ним ограничения при беспроводном подключении к системе управления	PT ISIM позволяет идентифицировать и сообщать обо всех несанкционированных или неавторизованных сетевых устройствах, выполняющих сетевое взаимодействие с компонентами системы управления, а также выполнять функции реагирования и ограничения сетевого взаимодействия на уровне сетевого узла	PT ISIM View Sensor, PT ISIM Collector, PT ISIM Endpoint Agent

Идентификатор требования	Название требования 62443 3-3	Содержание требования 62443 3-3	Покрытие требований функциональностью PT ISIM	Компонент PT ISIM
SR 2.2 (1)	Идентификация и отчет о несанкциони-рованных беспроводных устройствах	Система управления должна предоставлять возможность идентифицировать и сообщать о несанкционированных беспроводных устройствах, передающих в физической среде системы управления	PT ISIM позволяет идентифицировать и сообщать обо всех несанкционированных или неавторизованных сетевых устройствах, выполняющих сетевое взаимодействие с компонентами системы управления	PT ISIM View Sensor, PT ISIM Collector, PT ISIM Endpoint Agent
SR 2.5	Блокировка сессии	Система управления должна предоставлять возможность блокировки сессии автоматически после заданного периода неактивности или вручную	PT ISIM позволяет ограничивать сетевые сессии на отдельных сетевых узлах, включая возможность полной изоляции узла	PT ISIM Endpoint Agent
SR 2.6	Завершение удаленной сессии	Система управления должна предоставлять возможность завершать удаленную сессию автоматически после заданного периода неактивности или вручную	PT ISIM позволяет ограничивать сетевые сессии, включая удаленные сессии на отдельных сетевых узлах, в том числе обеспечивает возможность полной изоляции узла	PT ISIM Endpoint Agent
SR 2.7	Контроль одновременных сессий	Система управления должна предоставлять возможность ограни-чивать количество одновременных сессий на одном интерфейсе для любого пользователя	PT ISIM позволяет ограничивать сетевые сессии, включая одновременные сессии для любых пользователей на отдельных сетевых узлах, в том числе обеспечивает возможность полной изоляции узла	PT ISIM Endpoint Agent
SR 2.8	События, подлежащие аудиту	Система управления должна предоставлять возможность генерировать записи аудита, релевантные для безопасности (изменение контроля доступа, ошибки, системные события и т. д.)	PT ISIM обеспечивает сбор, обработку и анализ событий и записей журналов аудита операционных систем, прикладного программного обеспечения, а также ПЛК и сетевых устройств	PT ISIM View Sensor, PT ISIM Collector, PT ISIM Endpoint Agent
SR 2.8 (1)	Централизованно управляемый системный журнал аудита	Система управления должна предоставлять возможность централи-зованно управлять событиями аудита и собирать записи аудита из нескольких компонентов в единый журнал	При использовании PT ISIM в составе системы управления он позволяет организовать централизован-ный сбор, хранение, обработку и доступ к событиям и данным аудита	PT ISIM View Sensor, PT ISIM Collector, PT ISIM Endpoint Agent

Идентификатор требования	Название требования 62443 3-3	Содержание требования 62443 3-3	Покрытие требований функциональностью PT ISIM	Компонент PT ISIM
SR 2.9	Емкость хранения данных аудита	Система управления должна выделять достаточную емкость хранения записей аудита и предоставлять механизмы для снижения вероятности превышения емкости	PT ISIM имеет инструменты для гибкой настройки глубины хранения записей аудита в зависимости от типа и объема обрабатываемых данных	PT ISIM View Sensor
SR 2.9 (1)	Предупреждение при достижении порога емкости хранения данных аудита	Система управления должна предоставлять возможность выдавать предупреждение, когда объем хранения записей аудита достигает настраиваемого порога	При достижении пороговых значений объема хранения данных PT ISIM информирует об этом пользователей и выдает предупреждение в интерфейсе	PT ISIM View Sensor
SR 2.10	Ответ на сбои обработки данных аудита	Система управления должна предоставлять возможность предупреждать персонал и предотвращать нарушения работы основных служб при сбое обработки данных аудита	При использовании PT ISIM в составе системы управления в качестве централизованной системы хранения и обработки данных аудита безопасности пользователь имеет доступ к системе самодиагностики и контроля системных служб и сервисов, которая может информировать в том числе и о сбоях обработки данных аудита	PT ISIM View Sensor
SR 2.11	Временные метки	Система управления должна предоставлять временные метки при создании записей аудита	PT ISIM может обрабатывать записи аудита с метками времени, а также проставлять метки времени самостоятельно	PT ISIM View Sensor
SR 2.11 (2)	Защита целостности источника времени	Источник времени должен быть защищен от несанкциони-рованного изменения и должен вызывать событие аудита при изменении	PT ISIM позволяет обрабатывать события аудита при несанкционированном изменении конфигурационных параметров источника времени и информировать пользователя об этом событии в интерфейсе	PT ISIM View Sensor, PT ISIM Collector, PT ISIM Endpoint Agent
SR 2.12	Прослеживаемость действий пользователя	Система управления должна предоставлять возможность определять, совершил ли определен-ный пользователь конкретное действие	PT ISIM обеспечивает централизованный сбор, обработку и анализ событий и записей журналов действий пользователей с компонентов систем управления, позволяет определять выполнение конкретным пользователем конкретных действий или операций	PT ISIM View Sensor, PT ISIM Collector, PT ISIM Endpoint Agent

Идентификатор требования	Название требования 62443 3-3	Содержание требования 62443 3-3	Покрытие требований функциональностью PT ISIM	Компонент PT ISIM
SR 2.12 (1)	Прослеживаемость действий всех пользователей	Система управления должна предоставлять возможность определять, совершил ли конкретный пользователь (человек, программный процесс или устройство) конкретное действие	PT ISIM обеспечивает централизованный сбор, обработку и анализ событий и записей журналов всех компонентов и действий пользователей систем управления, позволяет определять выполнение конкретным компонентом или пользователем конкретных действий или операций	PT ISIM View Sensor, PT ISIM Collector, PT ISIM Endpoint Agent
SR 3.1	Целостность коммуникации	Система управления должна предоставлять возможность защищать целостность передаваемой информации	PT ISIM позволяет определять нарушения целостности передаваемой информации в сетевом трафике и на конечных узлах систем управления	PT ISIM View Sensor, PT ISIM Collector, PT ISIM Endpoint Agent
SR 3.2	Защита от вредоносного кода	Система управления должна предоставлять возможность использовать механизмы защиты для обнаружения и предотвращения действия вредоносного кода	PT ISIM включает полнофункциональные средства обнаружения и защиты от вредоносного кода	PT ISIM Endpoint Agent
SR 3.2 (1)	Защита от вредоносного кода на точках входа и выхода	Система управления должна предоставлять возможность использовать механизмы защиты от вредоносного кода на всех точках входа и выхода	PT ISIM предоставляет механизмы защиты от вредоносного кода как на уровне точек входа и выхода, так и на уровне сетевого взаимодействия	PT ISIM Endpoint Agent
SR 3.2 (2)	Центральное управление и отчетность для защиты от вредоносного кода	Система управления должна предоставлять возможность управлять механизмами защиты от вредоносного кода	PT ISIM предоставляет возможность централизованного управления механизмами защиты от вредоносного кода	PT ISIM View Sensor, PT ISIM Collector, PT ISIM Endpoint Agent
SR 3.3	Проверка функциональности безопасности	Система управления должна предоставлять возможность поддерживать проверку предполагаемой операции функций безопасности (FAT, SAT, плановое обслуживание)	При использовании PT ISIM в качестве встроенного решения для кибербезопасности система имеет возможность поддерживать проверки функций безопасности на всех этапах жизненного цикла (FAT, SAT, плановое обслуживание)	PT ISIM View Sensor, PT ISIM Collector, PT ISIM Endpoint Agent
SR 3.3 (1)	Автоматизированные механизмы для проверки функциональности безопасности	Система управления должна предоставлять возможность использовать автоматизированные механизмы для поддержки управления проверкой безопасности	PT ISIM включает функциональность автоматизированных проверок защищенности	PT ISIM View Sensor, PT ISIM Collector, PT ISIM Endpoint Agent

Идентификатор требования	Название требования 62443 3-3	Содержание требования 62443 3-3	Покрытие требований функциональностью PT ISIM	Компонент PT ISIM
SR 3.3 (2)	Проверка функциональности безопасности во время нормальной эксплуатации	Система управления должна предоставлять возможность поддерживать проверку предполагаемой операции функций безопасности во время нормальной эксплуатации	PT ISIM может использоваться в составе систем управления вместе с другими продуктами Positive Technologies для выполнения проверок функций безопасности во время нормальной эксплуатации	PT ISIM View Sensor, PT ISIM Collector, PT ISIM Endpoint Agent
SR 3.4	Целостность программного обеспечения и информации	Система управления должна предоставлять возможность обнаруживать, регистрировать, сообщать и защищать от несанкциони-рованных изменений ПО и информации	PT ISIM обнаруживает как сами факты изменения и модификации ПО или информации, так и попытки выполнения таких операций внутренними или внешними пользователями	PT ISIM View Sensor, PT ISIM Collector, PT ISIM Endpoint Agent
SR 3.4 (1)	Автоматизированное уведомление о нарушениях целостности	Система управления должна предоставлять возможность использовать автоматизированные инструменты для уведомления при обнаружении нарушений целостности	PT ISIM автоматически информирует пользователей при обнаружении фактов нарушения целостности ПО или информации	PT ISIM View Sensor, PT ISIM Collector, PT ISIM Endpoint Agent
SR 3.6	Детерминированный поток выходных сигналов	Система управления должна обеспечивать возможность приведения потоков выходных сигналов к заданному режиму, если в результате атаки не может поддержи-ваться штатное функционирование	PT ISIM позволяет установить и применить правила автоматического реагирования конечных узлов с выводом их в требуемое состояние или режим сетевого обмена при обнаружении атаки	PT ISIM Endpoint Agent
SR 3.8	Целостность соединений	Система управления должна защищать целостность соединений и отклонять недействительные идентификаторы соединений	PT ISIM позволяет установить и применить белые списки сетевых соединений на уровне сети и на уровне узла	PT ISIM View Sensor, PT ISIM Collector, PT ISIM Endpoint Agent
SR 3.8 (2)	Генерация уникального идентификатора сессии	Система управления должна предоставлять возможность генерировать уникальный ID сессии для каждой сессии	PT ISIM присваивает уникальный идентификатор каждому сетевому соединению	PT ISIM View Sensor, PT ISIM Collector

Идентификатор требования	Название требования 62443 3-3	Содержание требования 62443 3-3	Покрытие требований функциональностью PT ISIM	Компонент PT ISIM
SR 3.9	Защита информации аудита	Система управления должна защищать информацию аудита и инструменты аудита от несанкцио-нированного доступа, модификации и удаления	Информация аудита и встроенные инструменты могут быть защищены от несанкционированного доступа и модификации с помощью средства обнаружения реагирования на конечных узлах, в ходящего в состав функциональных компонентов PT ISIM	PT ISIM View Sensor, PT ISIM Collector, PT ISIM Endpoint Agent
SR 4.1	Конфиденциальность информации	Система управления должна предоставлять возможность защиты конфиденциальности информации, для которой поддерживается явная авторизация для осуществления операции чтения (при хранении или при передаче)	PT ISIM обнаруживает попытки нарушения конфиденциальности информации, выполняемые посредством неавторизованных операций чтения и записи при хранении на сетевых узлах (в покое) или при передаче (транзите)	PT ISIM View Sensor, PT ISIM Collector, PT ISIM Endpoint Agent
SR 4.1 (1)	Защита конфиденциальности информации в состоянии покоя или при передаче через недоверенные сети	Система управления должна предоставлять возможность защищать конфиденциальность информации в состоянии покоя и сессий удаленного доступа, проходящих через недоверенную сеть	PT ISIM обнаруживает попытки нарушения конфиденциальности информации, выполняемые посредством неавторизованных операций чтения и записи при хранении на сетевых узлах (в покое) или при передаче по каналам удаленного доступа, проходящим через внешние не доверенные сети	PT ISIM View Sensor, PT ISIM Collector, PT ISIM Endpoint Agent
SR 4.1 (2)	Защита конфиденциальности информации, переходящей через границы зон	Система управления должна предоставлять возможность защищать конфиденциальность информации, проходящей через любую границу зоны	PT ISIM обнаруживает попытки нарушения конфиденциальности информации, выполняемые посредством неавторизованных операций чтения и записи при передаче через границы сети системы управления	PT ISIM View Sensor, PT ISIM Collector, PT ISIM Endpoint Agent
SR 5.2	Защита границы зоны	Система управления должна предоставлять возможность мониторить и контролировать коммуникации на границах зон для обеспечения секционирования, определенного в модели зон и трактов, основанной на рисках	PT ISIM обеспечивает мониторинг сетевых коммуникаций внутри и на границах зон сетевых сегментов, и может гибко настраиваться для обнаружения нарушения зонирования и сетевого взаимодействия между сетевыми сегментами	PT ISIM View Sensor, PT ISIM Collector

Идентификатор требования	Название требования 62443 3-3	Содержание требования 62443 3-3	Покрытие требований функциональностью PT ISIM	Компонент PT ISIM
SR 5.2 (1)	Запрет по умолчанию, разрешение по исключению	Система управления должна предоставлять возможность запрещать сетевой трафик по умолчанию и разрешать сетевой трафик по исключению (так называемые операции deny all, permit by exception)	PT ISIM позволяет ограничить сетевой трафик в соответствии с требуемыми политиками безопасности на уровне сетевого узла	PT ISIM Endpoint Agent
SR 5.3	Ограничения общесетевой коммуникации между пользователями	Система управления должна предоставлять возможность предотвращать получение общесетевых сообщений между людьми от пользователей или систем, внешних по отношению к системе управления	PT ISIM позволяет ограничить передачу и получение пользователями сообщений общесетевых коммуникаций из внешних по отношению к системе управления сетей в соответствии с требуемыми политиками безопасности на уровне сетевого узла	PT ISIM Endpoint Agent
SR 5.3 (1)	Запрет общесетевой коммуникации между пользователями	Система управления должна предоставлять возможность предотвращать как передачу, так и получение общесетевых сообщений между пользователями	PT ISIM позволяет ограничить передачу и получение сообщений общесетевых коммуникаций внутри системы управления между пользователями в соответствии с требуемыми политиками безопасности на уровне сетевого узла	PT ISIM Endpoint Agent
SR 6.1	Доступность журнала аудита	Система управления должна предоставлять авторизованным пользователям и (или) системам возможность доступа к журналам аудита только для чтения	PT ISIM поддерживает интерфейсы и протоколы доступа к журналам аудита компонентов систем управления в режиме чтения и позволяет реализовать централизованный сбор данных из этих журналов и централизованный доступ к этим данным в интерфейсе для авторизованных пользователей	PT ISIM View Sensor
SR 7.7	Наименьшая функциональность	Система управления должна предоставлять возможность специально запрещать и (или) ограничивать использование неиспользуемых функций, портов, протоколов и (или) служб	PT ISIM позволяет ограничить использование избыточных или неиспользуемых функций, портов, протоколов или служб в соответствии с требуемыми политиками безопасности на уровне сетевого узла	PT ISIM Endpoint Agent

Идентификатор требования	Название требования 62443 3-3	Содержание требования 62443 3-3	Покрытие требований функциональностью PT ISIM	Компонент PT ISIM
SR 7.8	Инвентаризация компонентов системы управления	Система управления должна обеспечивать возможность предоставлять текущий список установленных компонентов и их связанных свойств	PT ISIM обеспечивает глубокую и полную инвентаризацию программных и аппаратных ресурсов системы управления и предоставляет актуальный список всех компонентов, их связанных свойств, журнал выполненных операций, авторизованных пользователей, профилирование сетевого трафика	PT ISIM View Sensor, PT ISIM Collector, PT ISIM Endpoint Agent

5. Заключение

Реализация положений стандарта ISA/IEC 62443 имеет **критическое значение для обеспечения киберустойчивости** систем промышленной автоматизации и операционных инфраструктур. В условиях современного ландшафта угроз, когда атаки на промышленные объекты становятся все более изощренными и деструктивными, базовых мер безопасности (таких как стандартные межсетевые экраны и антивирусы) уже недостаточно. Индустрии требуются профильные решения, способные надежно защищать АСУ ТП и отвечающие строгим требованиям к непрерывности технологических процессов.

Компания **Positive Technologies** целенаправленно создавала и продолжает активно развивать продукт **PT ISIM** именно для того, чтобы промышленные предприятия имели в своем распоряжении надежный, гибкий и полнофункциональный инструмент. Благодаря передовым технологиям глубокого анализа трафика, инвентаризации активов и выявлению инцидентов, PT ISIM позволяет организациям не только выполнять строгие технические и процессные требования (в том числе IEC 62443-3-3), но и обеспечивать реальную защищенность инфраструктуры от актуальных киберугроз.

positive technologies

Positive Technologies — лидер рынка 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. Наши технологии используют более 3300 организаций по всему миру, в том числе 80% компаний из рейтинга «Эксперт-400».

Positive Technologies — первая и единственная компания из сферы кибербезопасности на Московской бирже (MOEX: POSI), у нее более 185 тысяч акционеров.