Актуальные киберугрозы для российских промышленных предпрятий

ОГЛАВЛЕНИЕ

Об исследовании

В отчете описаны киберугрозы для российского промышленного сектора: рассматривается, чем промышленность отличается от других отраслей, как действуют злоумышленники, в том числе в технологическом сегменте сети, какие группировки атакуют промышленный сектор и какие методы атак используют, а также с какими последствиями сталкиваются предприятия и как защититься от их наступления.

Среди анализируемых промышленных предприятий — компании из сектора энергетики и ТЭК, машиностроения, металлургии, приборостроения, добывающей, обрабатывающей, химической, фармацевтической, легкой, космической, пищевой, авиа- и агропромышленности, а также различные производственные компании (заводы, фабрики и т. п.).

Представленные данные и выводы основаны на собственной экспертизе компании Positive Technologies, данных экспертного центра безопасности PT Expert Security Center (PT ESC), на материалах, полученных от центра промышленной экспертизы Positive Technologies, на результатах расследований, анализа объявлений на специализированных дарквеб-площадках, проведенного направлением аналитических исследований PT Cyber Analytics, на информации, полученной из отчетов с кибербитв Standoff, на данных, основанных на экспертизе PT ISIM, а также на информации из авторитетных открытых источников.

Наша база инцидентов регулярно обновляется. Следует отметить, что информация о некоторых событиях может поступать значительно позже фактического времени кибератаки. В отчете представлены данные, охватывающие период с 2024 по 2025 год – за это время на российскую промышленность обрушилась волна атак злоумышленников. В исследование не включены данные за I квартал 2026 года, поскольку они могут не в полной мере отражать общую динамику, а также в связи с использованием подхода, предполагающего сопоставление с аналогичными цельными периодами.

По нашей оценке, большинство кибератак не предается огласке из-за репутационных рисков. Вследствие этого подсчитать точное число угроз не представляется возможным даже для организаций, занимающихся расследованием инцидентов и анализом действий хакерских группировок. В нашем отчете каждая массовая атака (например, фишинговая рассылка множеству адресатов) рассматривается как одна отдельная, а не как несколько. Мы учитываем только успешные кибератаки (инциденты), которые привели к негативным последствиям для компании. Термины, которые мы использовали в исследовании, приведены в глоссарии на сайте Positive Technologies.

Резюме

- За последние два года российская промышленность стала приоритетной целью для злоумышленников: отрасль занимала первое место по числу инцидентов (16% успешных атак в России в 2024-м, 19% — в 2025-м).

- В целом мировой промышленный сектор уникален с точки зрения социально-экономического и технологического ландшафта. В России интерес злоумышленников к промышленности обусловлен некоторыми специфичными факторами: геополитической напряженностью; влиянием статуса России как энергетической державы; уходом из страны в 2022 году западных вендоров ИТ-решений; дефицитом специалистов по информационной безопасности.

- Основными методами кибератак на отечественные промышленные предприятия в 2024–2025 годы оставались использование вредоносного программного обеспечения (ВПО) и применение социальной инженерии. По сравнению с 2022 и 2023 годами доля успешных атак с применением ВПО выросла с 56 до 83%; доля атак с использованием методов социальной инженерии — с 49 до 71%.

- Доля успешных кибератак, связанных с компрометацией цепочки поставок и доверенных каналов связи, в 2024–2025 годах в России (4%) вдвое превышала общемировой показатель (2%). Ситуация показывает, что отечественные промышленные компании особо уязвимы в областях, где есть взаимодействие с партнерами.

- Распределение типов ВПО, используемого в атаках на промышленность в России за последние два года, существенно отличалось от общемирового. Для страны характерна высокая доля применения ВПО для удаленного управления (55%) и шпионского ПО (33%), в то время как в мире главной киберугрозой остаются шифровальщики (54%).

- За рассматриваемый период 55 группировок[1] совершили атаки на российский производственный сектор. Самыми активными являются кибершпионские структуры: они провели 47% атак на отрасль[2], при этом было зафиксировано не менее 22 таких группировок. В 92% случаев кибершпионские группы применяли ВПО, как минимум две трети (68%) пользовались инструментами собственной разработки.

[1] Фактическое число группировок, атаковавших российские промышленные предприятия, может быть выше.
[2] Здесь и далее, рассматриваются только те случаи, в которых можно судить о мотивации злоумышленников..

- Более четверти (28%) успешных атак на российские промышленные компании совершены хактивистами, чьей главной задачей было полное разрушение скомпрометированной инфраструктуры. Инструментами для этого становились шифровальщики (80% атак с применением ВПО) и ПО, удаляющее данные (60% атак с применением ВПО).

- Пятая часть (25%) инцидентов вызвана действиями финансово мотивированных преступников. Основными целями атакующих становились получение выкупа и кража конфиденциальных данных с последующей монетизацией. Для реализации планов более чем в трети (35%) случаев применялись шифровальщики, почти в двух третьих (62%) — ВПО для удаленного управления.

- Наиболее опасной частью атаки на промышленное предприятие являются действия злоумышленников в технологическом сегменте, однако их описание редко становится публичным в силу репутационных рисков и секретности сведений о конфигурации производственных систем. Дополнительный риск для OT-сегмента[3] — ограниченный выбор инструментов для защиты: требуются специализированные решения, совместимые с промышленным оборудованием и учитывающие особенности производственных процессов.

- По данным Zero Networks, 75% атак на OT начинаются с компрометации ИТ-инфраструктуры. Другие способы получения доступа к технологическому сегменту — атаки через подрядчиков, а также из контура самой компании, например в результате подключения зараженного запоминающего USB-устройства к АРМ.

- После получения первоначального доступа к технологическому сегменту злоумышленники переходят к разведке на уровне сети, затем — к повышению привилегий и обходу авторизации. Следующие шаги — подготовка инструментов и непосредственное воздействие на технологический процесс. Каждый из этих этапов можно обнаружить при помощи средств защиты информации.

- Атаки на отечественные производственные компании в 2024–2025 годах преимущественно заканчивались утечками конфиденциальных сведений (61%) и нарушением основной деятельности (33%). Чаще всего из организаций похищали информацию, составляющую коммерческую тайну (29%): доля ее краж существенно превышает общероссийский показатель по всем отраслям (на 10 п. п.). В 23% утечек из промышленных предприятий фигурировали учетные данные, в связи с чем можно предположить: в 2026–2027 годах возрастет число кибератак, в которых эти сведения будут использованы.

[3] Операционные технологии (OT) — аппаратное и программное обеспечение, используемое для мониторинга работы физических процессов, устройств и инфраструктуры и для управления ими.

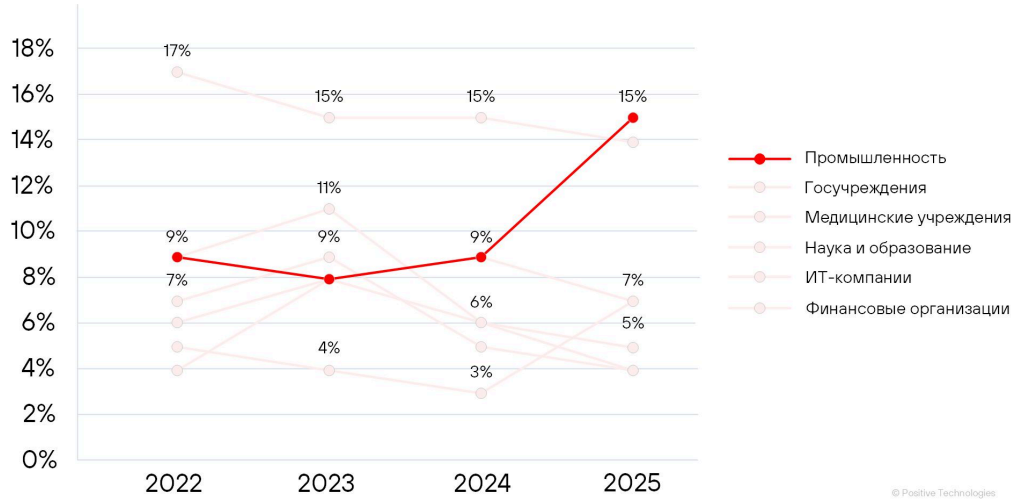
- На теневых площадках более половины (52%) объявлений об утечках из российских промышленных организаций связаны с бесплатной раздачей украденных данных, при этом значительная часть из них (73%) — небольшого объема (до 1 ГБ). Седьмая часть сообщений на форумах (14%) связана с продажей украденной информации, в двух третьих случаев размер утечки был существенным — от 100 тыс. до 1 млн записей.

- По мере цифровизации предприятий и роста связности между ИТ- и ОТ-сегментами требования к безопасности смещаются от защиты отдельных систем к обеспечению киберустойчивости производственной среды в целом — защищать только корпоративную инфраструктуру недостаточно. Промышленным компаниям необходимы не только базовые меры ИБ, но и специализированные решения: они позволяют выстраивать защиту технологического сегмента — выявлять риски на ранних этапах, реагировать на киберинциденты в производственной среде и определять логику атак (в случае ретроспективного анализа).

Введение

На протяжении многих лет промышленность не выходит из первой пятерки отраслей по количеству киберинцидентов, а в недавнее время на сегмент обрушилась волна атак злоумышленников, и он впервые обогнал традиционно лидирующий в этом списке госсектор.

Рисунок 1. Категории жертв среди организаций в мире (2022–2025)



Аналогичная картина наблюдается и в России: за последние два года промышленный сектор чаще остальных подвергался натиску со стороны киберпреступных группировок. По сравнению с 2023 годом прирост доли атак в 2024 году составил 5 п. п., в 2025 году — 8 п. п.

Рисунок 2. Доля атак на промышленные организации в России и мире (от общего числа атак на организации, 2022–2025)

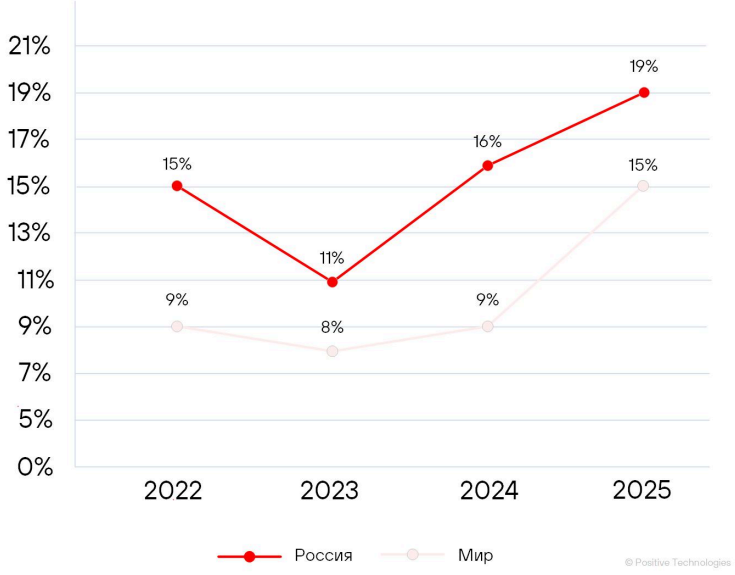
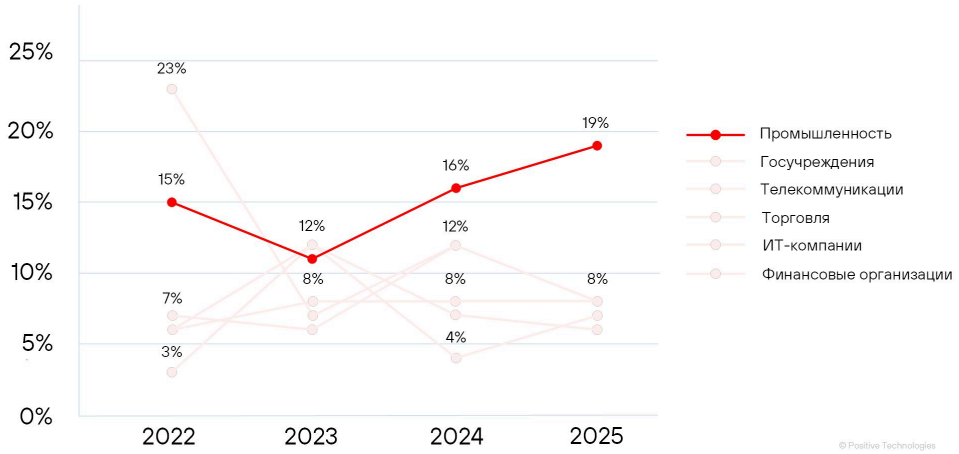


Рисунок 3. Категории жертв среди российских организаций (2022–2025)



Специфика промышленного сектора как цели кибератак

Уникальный социально-экономический ландшафт

Промышленный сектор играет ключевую роль в развитии страны, является одним из главных драйверов экономического роста. Так, по данным Всемирного банка, в 2024 году российская промышленность увеличила свой вклад в ВВП на 6% — до 668 млрд долларов, что позволило стране занять пятое место в мире по объему вклада отрасли в национальную экономику. Производственные компании выступают источником рабочих мест, способствуют развитию региональной инфраструктуры. Так, по данным на 2025 год, только в Москве в промышленном сегменте было занято более 750 тыс. человек. Организации сектора создают основу для деятельности смежных отраслей, таких как транспорт и логистика, строительство и торговля.

Промышленные предприятия обеспечивают государство жизненно необходимыми ресурсами: энергией и сырьем, стройматериалами, машинами и оборудованием. Нарушение деятельности даже одной организации способно привести к дефициту товаров и услуг, что сказывается на социально-экономической ситуации в стране.

Показательный случай произошел с британским производителем автомобилей Jaguar Land Rover в августе 2025 года: в результате кибератаки по всему миру отключились ИТ-системы компании и остановились производственные операции. Многим из 33 тыс. сотрудников было сказано оставаться дома. Дилерские системы работали с перебоями, компании пришлось отменять или откладывать заказы комплектующих. Как следствие, часть поставщиков оказалась на грани банкротства. По некоторым оценкам, инцидент обошелся британской экономике примерно в 2,55 млрд долларов и затронул более 5 тыс. организаций.

Организации сектора являются носителями критически важной информации — производственных рецептур, инженерных решений и других ноу-хау. Утечка может обеспечить конкурентам преимущество, позволить им пропустить годы исследований, ускорить копирование технологий. Кроме того, эти сведения помогают понять, каковы реальные технические возможности предприятия и отрасли в целом.

Отличие кибератак на промышленный сектор заключается в том, что они оказывают прямое воздействие на физические процессы, а их последствия выходят за рамки цифрового пространства. Инциденты могут привести не только к нарушению производства, но и к катастрофам, влияющим на жизнь и здоровье населения, экологию и критически важную инфраструктуру.

Уникальный технологический ландшафт

Для промышленных предприятий время безотказной работы — это приоритет: даже кратковременная остановка производства может привести к экономическим потерям, нарушению сроков поставок и срыву производственного плана. Согласно отчету Siemens за 2024 год, незапланированные простои обходятся компаниям из списка Fortune Global 500 в 11% от их годового оборота — почти в 1,4 трлн долларов. Поэтому, в отличие от других отраслей, где безопасность строится по модели «конфиденциальность — целостность — доступность», в промышленности акцент делается на доступности и стабильности процессов. Такая приоритизация влияет на набор допустимых мероприятий по обеспечению безопасности: защитные меры, требующие регулярного перезапуска, откладываются, циклы обновлений замедляются. Часто компании предпринимают лишь компенсирующие меры или продолжают пользоваться уязвимым ПО, пока риск остановки процессов перевешивает страх перед кибератакой.

В сравнении с ИТ-системами, обновление которых происходит каждые несколько лет, ОТ-активы имеют более длительный жизненный цикл, охватывающий десятилетия. Они используются для управления физическим оборудованием, сертификация обходится дорого, а в случае их модификации есть риск остановки производственных процессов, критически важных для предприятий. Кроме того, многие операционные технологии были спроектированы еще задолго до появления современных стандартов кибербезопасности. В результате возникают дополнительные проблемы:

- Зависимость от производителей и необходимость соблюдать требования к сертификации часто замедляют или вовсе блокируют обновление: любые изменения должны проходить сложную проверку на безопасность и на соответствие регламентам.

- Современные средства защиты не всегда совместимы со старыми системами управления, поэтому компании не могут «просто поставить антивирус».

Ситуация осложняется тем, что модернизация промышленной инфраструктуры требует значительных финансовых вложений. Кроме того, на больших объектах заменить отдельные компоненты не всегда возможно без комплексной реконструкции всей системы, что также влияет на выбор в пользу устаревших продуктов. В результате получается замкнутый круг: ограниченные ресурсы препятствуют модернизации, устаревшие системы повышают вероятность атак, а чтобы устранить последствия киберинцидентов, требуются еще бóльшие затраты, что сокращает возможности для обновления инфраструктуры.

С другой стороны, согласно концепции индустрии 4.0, с промышленными процессами все чаще интегрируются интеллектуальные цифровые технологии: IIoT, ИИ и решения, связанные с большими данными. Так, Минэнерго России сообщило, что более половины (58%) компаний ТЭК к концу 2025 года внедрили технологии ИИ, а к 2027 году искусственный интеллект будут применять 70% организаций отрасли. По данным исследования Strategy Partners, на 2024 год количество российских промышленных предприятий, использующих IIoT, достигло 7,1% (в 2020-м показатель составлял 4,5%), ML и big data (машинное обучение и большие данные) — 5,5% (в 2020-м — 2,1%). Инициативы направлены на повышение эффективности, гибкости и конкурентоспособности предприятий, однако поверхность атаки значительно расширяется.

О том, как злоумышленники могут атаковать промышленный интернет вещей, мы подробно рассказывали в нашем исследовании «Киберугрозы для промышленности: industrial IoT».

Зачастую современные технологии внедряются поверх существующей инфраструктуры, без ее комплексной модернизации. В результате формируется гибридная среда, в которой новейшие разработки сосуществуют с устаревшими компонентами, и обеспечение прозрачности процессов, соблюдение единых стандартов защиты становятся одними из самых сложных задач.

По описанным причинам для многих промышленных предприятий цифровизация это не только источник возможностей, но и дополнительный фактор риска. В подобных условиях основополагающая задача — сделать так, чтобы расширение технологических возможностей сопровождалось обеспечением видимости, управляемости и защищенности инфраструктуры.

Российская промышленность как цель для кибератак

Интерес злоумышленников к российской промышленности обусловлен не только вышеперечисленными факторами, но и рядом других причин. Одна из них – геополитическая напряженность. К примеру, промышленный сектор атакуют как шпионские и финансово мотивированные группировки, действия которых не всегда связаны с обострением международных отношений, так и хактивисты, руководствующиеся идеологическими, политическими или социальными мотивами. По данным нашего исследования, приоритетной целью хактивистов в период с июля 2024-го по конец сентября 2025-го были производственные компании.

Существенное влияние на формирование ландшафта киберугроз оказывает статус России как ведущей энергетической державы: страна полностью обеспечивает внутренний рынок энергоресурсами, развивает собственные технологии, выполняет экспортные обязательства. Стратегическая значимость отрасли не только усиливает ее влияние на мировой рынок, но и повышает интерес к ней со стороны различных групп киберпреступников — от злоумышленников, ищущих финансовую выгоду, до организованных и геополитически мотивированных субъектов, стремящихся воздействовать на экономическую стабильность через вмешательство в критически важные процессы. Об этом свидетельствуют и наши данные: отечественные энергетический сектор и ТЭК чаще остальных отраслей промышленности подвергались кибератакам в 2024–2025 годах (22%).

Рисунок 4. Атакованные секторы промышленности в России (2024–2025)

Вторым наиболее атакуемым сектором отечественного производства стало машиностроение (10%). Интерес злоумышленников может быть вызван активным развитием отрасли. Так, по данным Минпромторга, несырьевой неэнергетический экспорт (ННЭ) России в 2025 году показал положительную динамику, а машиностроение стало одной из ведущих отраслей: объем экспорта вырос примерно на 27%.

После ухода западных вендоров ИТ-решений с российского рынка в 2022 году более 80% предприятий столкнулись с проблемами в поставках: с увеличением сроков, невозможностью обновления ПО и прекращением технической поддержки. Компании были вынуждены оперативно искать и внедрять отечественные альтернативы — импортозамещение происходило в сжатые сроки, без полноценного тестирования и оценки рисков, что повысило вероятность ошибок и повлияло на возникновение уязвимостей. Однако по состоянию на конец 2025 года более половины субъектов КИИ[4] так и не перешли на отечественные продукты. По данным на 2024 год, импортозамещение ИТ-решений в промышленности оказалось в среднем на уровне 31%. Поддержка и обновление западных решений могут быть полностью или частично прекращены — в результате для киберпреступников открывается возможность эксплуатации неустраненных известных уязвимостей.

Влияет и дефицит специалистов по кибербезопасности в промышленном секторе: по некоторым данным, с января по август 2025 года спрос на экспертов в этой области вырос в машиностроении на 40% год к году, в энергетике — на 64%, в производстве непищевых товаров — на 85%.

С учетом всех факторов можно прогнозировать, что количество кибератак на промышленные организации в России в ближайшие годы не снизится. Важной задачей для промышленных организаций является построение надежной системы защиты, и это невозможно без знаний о тенденциях в сфере ИБ.

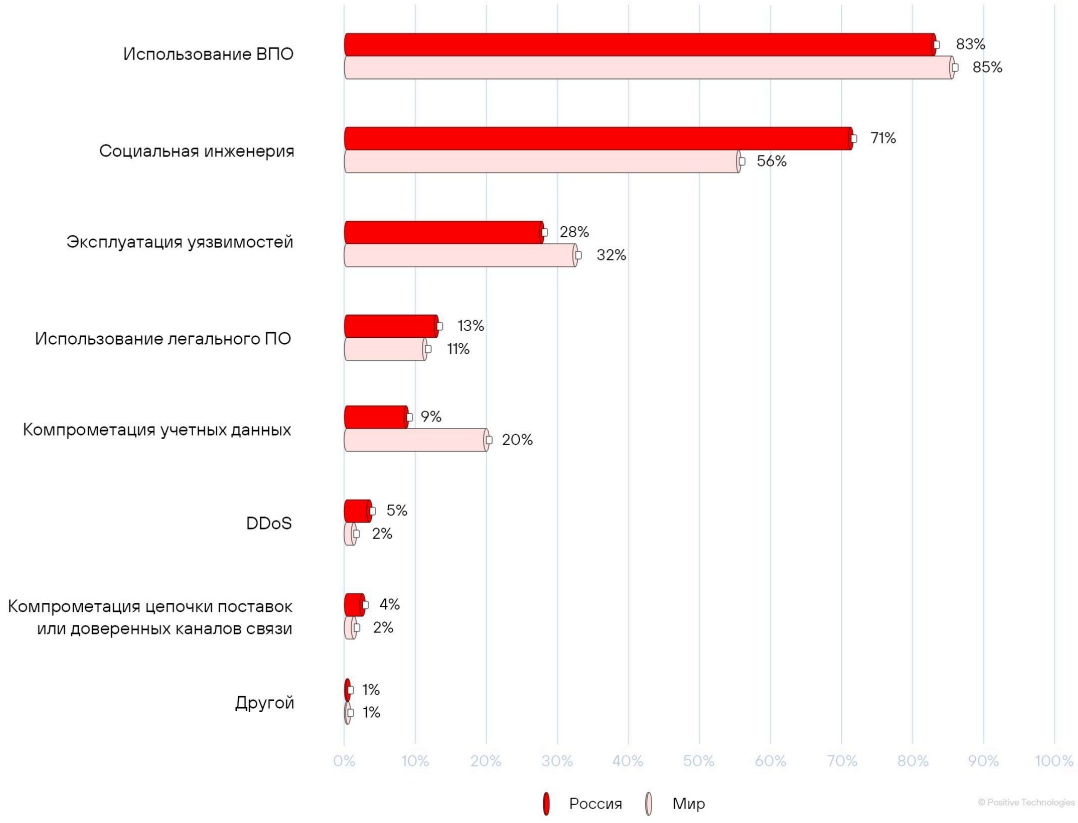
[4] К субъектам КИИ относят организации не только из сферы промышленности, но и из сегмента здравоохранения, связи, транспорта, науки, финансов и других.

Кто и как атакует российскую промышленность

Методы атак

Основными методами кибератак на промышленные предприятия в России, как и во всем мире, по-прежнему остаются использование вредоносного ПО и применение социальной инженерии. По сравнению с 2022–2023 годами их распространенность заметно возросла: доля инцидентов с применением ВПО увеличилась с 56 до 83%, с использованием социальной инженерии — с 49 до 71%.

Рисунок 5. Методы атак на промышленные организации в России и мире (доля успешных атак, 2024-2025)

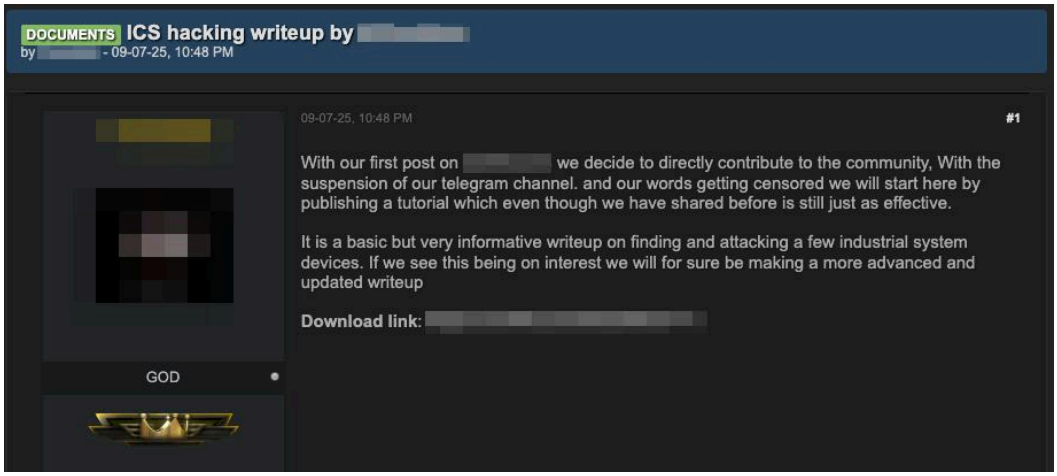


Одна из причин продолжающегося роста использования ВПО в атаках — это активное развитие теневого рынка: злоумышленникам больше не нужно тратить время на разработку вредоносов — их можно как купить или взять в аренду, так и спроектировать под заказ. По данным нашего исследования, посвященного рынку киберпреступности, медианная цена инфостилера составляет 400 долларов, ВПО для удаленного управления — 1,5 тыс. долларов, а шифровальщика — 7,5 тыс. долларов. Это позволяет каждому найти инструмент, который наилучшим образом соответствует целям и финансовым возможностям. Так, в атаках на отечественную промышленность

нередко использовалось коммерческое ВПО, среди которого наиболее распространенным было Remcos. По нашим данным, это семейство с 2023 года остается в десятке самых популярных[5].

Теневые форумы служат источником не только инструментов для кибератак, но и знаний, особенно полезных для начинающих злоумышленников. Так, на одном из ресурсов было обнаружено руководство по кибератакам на промышленные устройства.

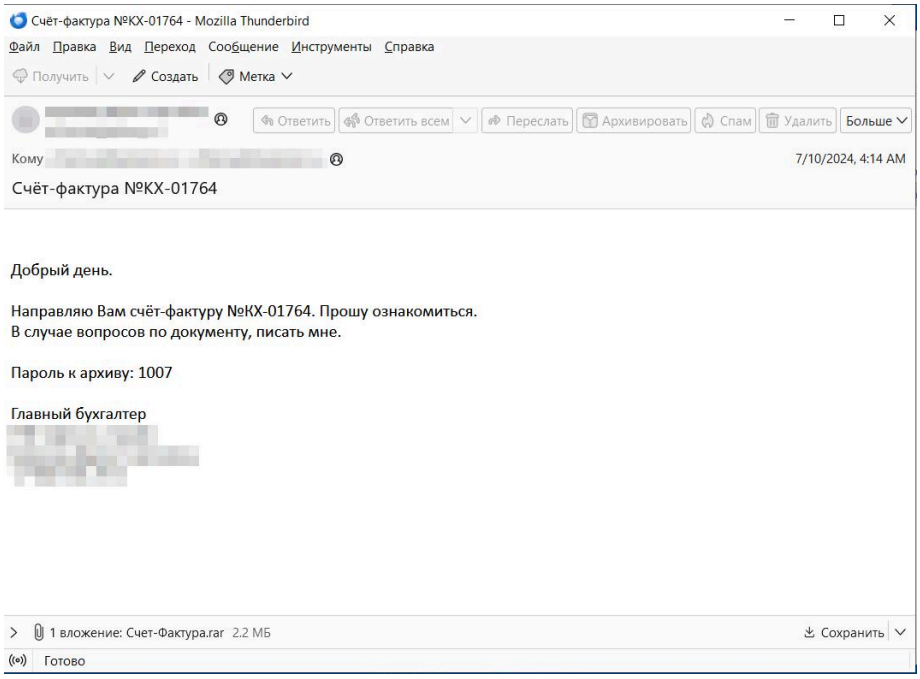
Рисунок 6. Раздача руководства по атакам на промышленные устройства



Основным каналом социальной инженерии в успешных атаках на российские промышленные организации была электронная почта (98%). Наиболее часто злоумышленники маскируют фишинговые приманки под вложения, связанные с рабочей деятельностью, а сами представляются сотрудниками атакуемой компании или организации из той же или смежной отрасли. Их письма могут восприниматься как легитимные — получатель меньше сомневается и реже проверяет отправителя. Так, летом 2024 года специалисты PT ESC обнаружили рассылку от группировки PhantomCore в адрес промышленной компании: преступники распространяли поддельную счет-фактуру. Во вложении находился защищенный паролем архив — это излюбленный прием злоумышленников, помогающий им обойти средства защиты электронной почты. Целью кампании было заражение устройства жертвы ВПО для удаленного управления — PhantomRAT.

[5] На основании данных, полученных при помощи PT Sandbox — в результате анализа вредоносных программ на территории России.

Рисунок 7. Рассылка от группировки PhantomCore (источник: PT ESC)

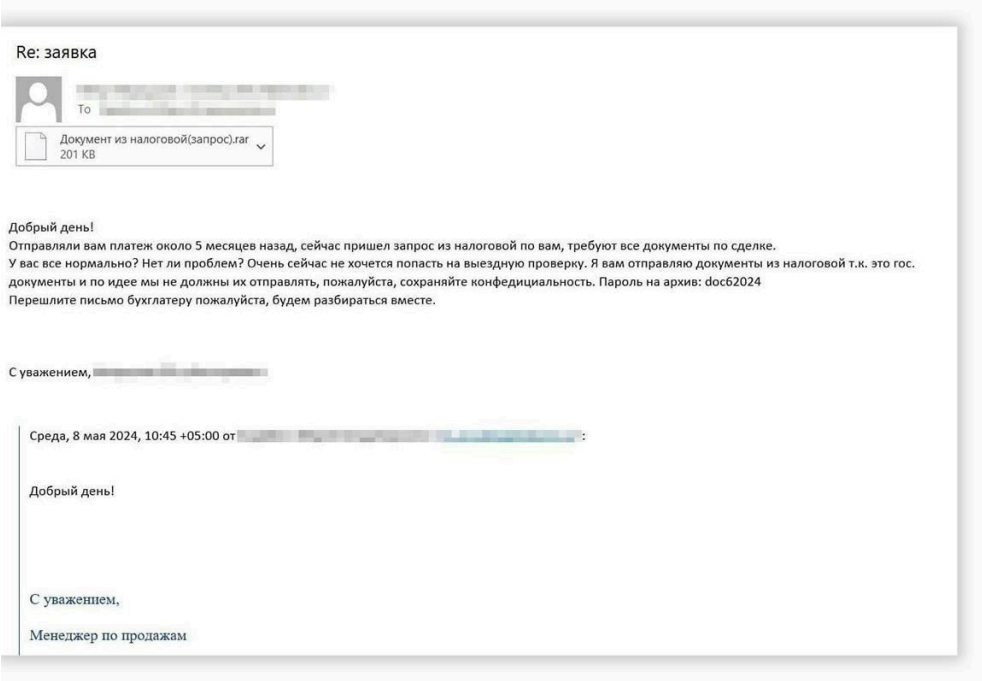


Для проведения подобных атак преступники могут регистрировать фишинговые домены — это позволяет им создавать почтовые адреса, максимально похожие на адреса лиц, за которых они себя выдают. Встречаются и случаи, когда злоумышленники используют аккаунты легитимных пользователей, с которыми у жертвы могла быть связь. Например, в ходе предотвращенной при помощи PT Sandbox кибератаки на российские оборонные и промышленные организации все та же PhantomCore задействовала скомпрометированную учетную запись для распространения архивов-полиглотов.

Преступники используют не только аккаунт, но и переписки жертвы во вредоносных целях — то есть применяют технику email thread hijacking (перехват ветки сообщений). Такой случай описали специалисты PT ESC: в ходе кибератаки на производителя стройматериалов группировка Hive0117 воспользовалась взломанным аккаунтом, отправив ответ на настоящее письмо из прошлого. Цель кампании — доставка на устройство жертвы ВПО DarkWatchman.

[6] Файл-полиглот — это файл, относящийся сразу к нескольким типам и работающий по-разному в зависимости от приложения, в котором он запущен.

Рисунок 8. Фишинговое письмо, отправленное группировкой Hive0117 (источник: PT ESC)



Другой популярной фишинговой приманкой в атаках на промышленность были сообщения, отправленные якобы от государственных органов. В этом случае механизм воздействия — это уважение к авторитету и страх перед последствиями, которые могут наступить, если оставить письмо без ответа. Например, в рамках целевой атаки на машиностроительное предприятие злоумышленники отправляли письма от имени СК РФ с вредоносным вложением в виде WhiteSnake Stealer.

Более чем в четверти (28%) инцидентов на отечественных производственных предприятиях преступники эксплуатировали уязвимости, в числе которых были и трендовые. Так, группировка PhantomCore задействовала уязвимость PT-2024-7974, о которой мы рассказывали в дайджесте в ноябре 2024 года, а злоумышленники QuietCrabs и Thor использовали недостаток, рассмотренный в августовском дайджесте, — PT-2025-30160 — для получения первоначального доступа.

В каждой восьмой кибератаке (13%) киберпреступники прибегали к использованию легитимного ПО. В частности, выбор злоумышленников нередко падал на инструменты для удаленного мониторинга и управления (RMM). Тенденцию мы отмечали в исследовании, основанном на данных пилотных проектов PT NAD, проведенных за второе полугодие 2024-го и первое полугодие 2025 года. По полученным данным, сетевая активность такого ПО была выявлена в 85% организаций. Подобные классы решений обычно не воспринимаются антивирусными средствами защиты как вредоносные, а злоумышленники могут использовать их в качестве альтернативы RAT-троянам. В свой арсенал RMM добавили такие группировки, как Bearlyfy, PhantomCore, PseudoGamaredon и другие.

Доля инцидентов, связанных с компрометацией цепочки поставок и доверенных каналов связи, в России (4%) вдвое превышает общемировую величину (2%). И хотя этот показатель остается сравнительно небольшим, ситуация сигнализирует: отечественные промышленные компании особо уязвимы в областях, где есть взаимодействие с партнерами. Так, к атакам через подрядчиков прибегали группы IAmTheKing, Hellhounds и MorLock.

Кроме того, одна компания нередко имеет прямой доступ к инфраструктуре и внутренней информации десятков клиентов. Для хактивистов это возможность одним ударом парализовать работу сразу нескольких организаций или даже целой отрасли, для финансово мотивированных групп — кратно увеличить заработок, для кибершпионов — собрать большое количество разведданных. Дополнительно — доступ через партнера выглядит легитимным, что создает условия для длительного скрытого присутствия злоумышленника в инфраструктуре жертвы.

В России каждый десятый (9%) киберинцидент в секторе производства связан с компрометацией учетных данных. Однако метод применялся более чем в два раза реже, чем в мировой практике. Относительно невысокая доля его использования может быть связана с с переосмыслением вопросов ИБ в российских компаниях — об этом сообщили почти две третьих (64%) опрошенных топ-менеджеров. Одновременно ужесточились требования регуляторов к обеспечению безопасности КИИ. В результате на предприятиях были внедрены как минимум базовые меры защиты, в том числе, например, MFA-технологии (по данным Сбера, наиболее активно они внедряются в финансовом секторе, нефтегазовой отрасли, промышленности и энергетике). Но уменьшение числа случаев компрометации учетных данных может оказаться временным, поскольку услуги брокеров первоначального доступа (initial access broker) не теряют своей популярности, а даже наоборот: по некоторым сведениям, за 9 месяцев 2025 года спрос на них вырос на 20% по сравнению с аналогичным периодом прошлого года.

Таким образом, число инцидентов, связанных с получением доступа к инфраструктуре через легитимные каналы связи (скомпрометированные учетные данные, системы подрядчиков), остается значительным. Это свидетельствует о том, что наличие формального периметра или даже сегментации сети само по себе не гарантирует защищенности, если у предприятия нет видимости связей, активности и изменений внутри инфраструктуры.

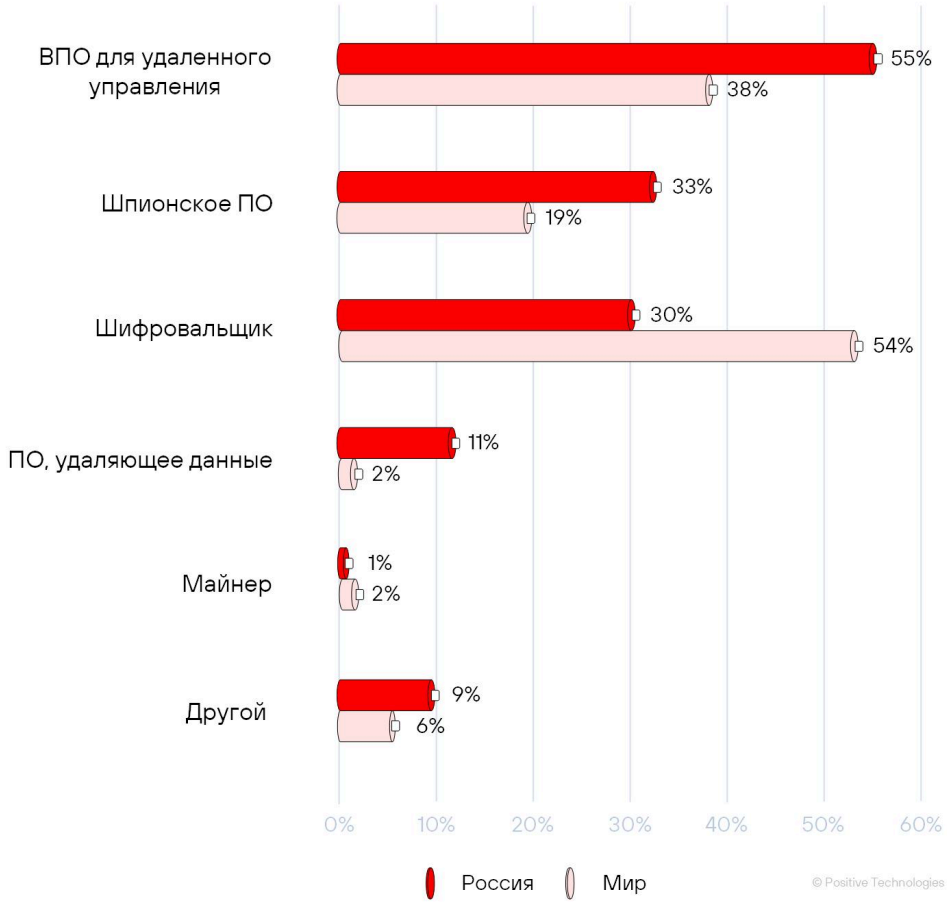
Доля DDoS-атак на промышленные организации в России (5%) более чем в два раза выше, чем во всем мире (2%). Мы связываем это с высокой активностью хактивистских групп, которые предпочитают быстрые и демонстративные методы воздействия. Однако количество DDoS-атак все же остается относительно невысоким. Причиной может быть то, что киберпреступники выбирают более заметные способы влияния. Кроме того, многие российские организации внедрили защиту от таких атак, что снизило их привлекательность для злоумышленников. По данным опроса,

проведенного компанией «ОБИТ» совместно с DDoS Guard, более чем в трех четвертях организаций (77%) в какой-либо мере была организована защита от DDoS-атак.

Вредоносное ПО

В то время как во всем мире шифровальщики остаются киберугрозой номер один для промышленных предприятий (54%), в России на первом месте находится ВПО для удаленного управления: оно применялось более чем в половине успешных кибератак с использованием ВПО (55%). Заметно отличается от мировой статистики и доля применения шпионского ПО: инструмент был задействован в каждой третьей атаке с использованием ВПО в России (33%) и менее чем в каждой пятой — в мире (19%). Все это может указывать на то, что приоритетными задачами для злоумышленников являются долгосрочное пребывание в инфраструктуре и сбор данных, а не немедленное вымогательство.

Рисунок 9. Типы вредоносного ПО в России и мире (доля успешных атак на промышленный сектор с использованием ВПО, 2024–2025)



Почти треть (30%) успешных атак с применением ВПО на российские промышленные организации совершена с использованием шифровальщиков. В мире большая часть инцидентов с применением этого типа ВПО (по нашим оценкам, около 90%[7]) связана с финансовой мотивацией киберпреступников, однако в России как минимум половина (более 50%) имеют хактивистскую направленность. Встречаются случаи, когда политически мотивированные преступники не просто шифруют информацию, но и оставляют сообщения с требованием выкупа. Один из таких примеров — атака группировки BO Team на российскую организацию из производственного сектора. Инцидент парализовал основные бизнес-процессы компании: были приостановлены отгрузки, прекратился прием заказов, из личных кабинетов клиентов исчезли данные. За возвращение контроля над системами преступная группировка запросила 50 тыс. долларов. По сообщениям злоумышленников, компания выплатила им требуемую сумму, однако ключи для дешифрования отправлены не были.

Высокую концентрацию хактивистов в стране также подтверждает большая относительно мировых данных доля использования ПО, удаляющего данные, — почти в каждой десятой атаке с применением ВПО (11%).

Около четверти (22%) инцидентов в российском промышленном секторе были вызваны использованием загрузчиков — этот показатель несколько превышает среднюю долю их использования в мире (на 6 п. п.). Предпочтения киберпреступников отражают усложнение кибератак на отечественные организации: загрузчики применяются для многоэтапного развертывания вредоносного ПО с целью затруднить обнаружение и анализ угрозы. Так, описанная специалистами PT ESC группировка QuietCrabs применяла загрузчик KrustyLoader, основная функция которого — расшифровать ссылку, ведущую на скачивание полезной нагрузки, загрузить ее, внедрить в целевой процесс и запустить.

Группировки, атаковавшие промышленные организации

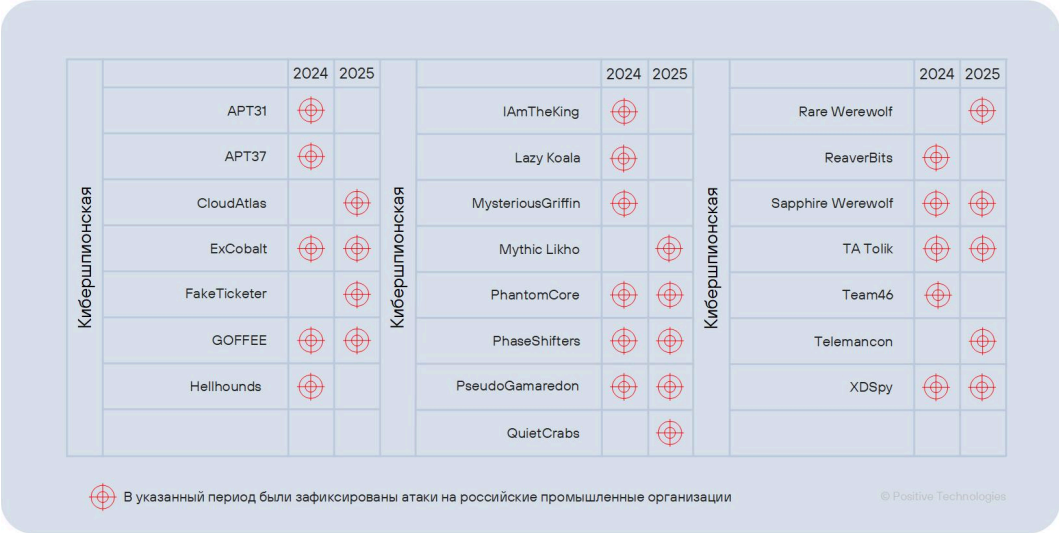
Многие из рассматриваемых в этом разделе группировок подробно описывались в нашем исследовании «CODE RED 2026: актуальные киберугрозы для российских организаций».

[7] Не всегда из описания новости можно однозначно судить о мотивации киберпреступников.

Кибершпионские группировки

Бóльшая часть атакующих — это государственно поддерживаемые кибершпионские структуры: в период с 2024 по 2025 год на российские промышленные предприятия были нацелены как минимум таких 22 группы. На их долю пришлось 47% всех атак. Некоторые группировки были активны на протяжении всего рассматриваемого периода.

Рисунок 10. Атаки кибершпионских группировок на российские промышленные предприятия (2024–2025)



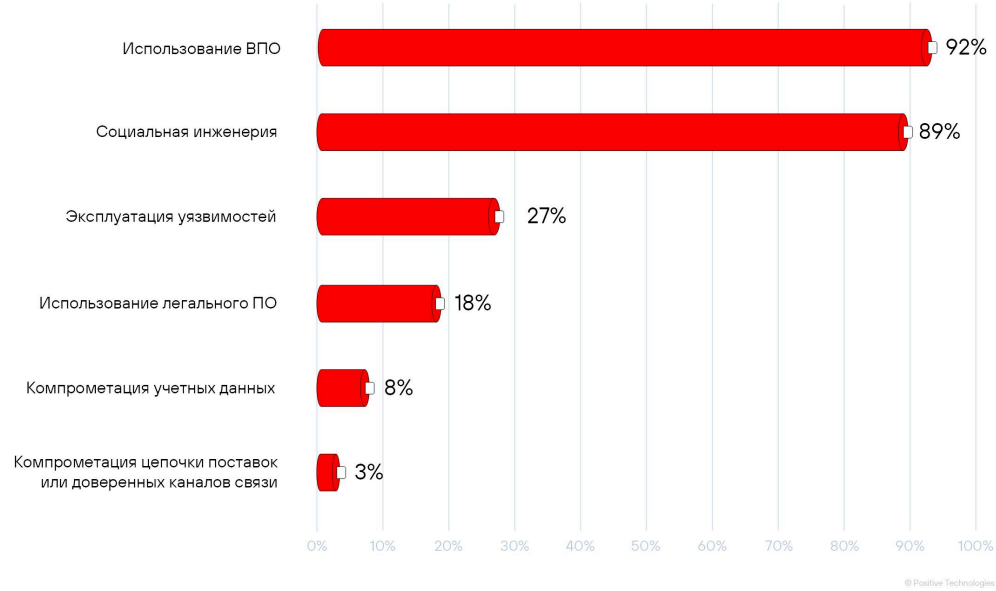
Основная цель кибершпионских группировок не быстрый эффект или деньги, а технологические знания и ноу-хау — стратегически ценная информация с промышленных объектов. Наиболее часто такие группы интересовались сектором энергетики и ТЭК, а также космической и авиапромышленностью.

Получив доступ к промышленным системам, злоумышленники также могут изучить инфраструктуру и потенциальные точки воздействия. Даже если атака не приведет к немедленным последствиям, полученные данные могут создать задел на будущее. Особую опасность представляет то, что инфраструктура многих производителей остается неизменной на протяжении длительного времени.

Промышленный сектор тесно связан с другими отраслями экономики. Часто наблюдение за одной организацией позволяет злоумышленникам собрать информацию о смежных сферах, что значительно расширяет разведывательные возможности.

Излюбленными методами атак кибершпионских групп на промышленные предприятия в России являются применение социальной инженерии (89%) и использование ВПО (92%). Как минимум две трети (68%) злоумышленников применяли инструменты собственной разработки — например, так поступали группировки ExCobalt, PhantomCore и Goffee: подход позволяет повысить скрытность, снизить вероятность обнаружения и адаптировать атаки под конкретную инфраструктуру. Это отличает кибершпионские группировки от хактивистов и финансово мотивированных групп, которые чаще используют готовые решения и ориентируются на быстрый результат.

Рисунок 11. Методы атак кибершпионских групп на промышленные организации в России (доля успешных атак, 2024–2025)



После получения доступа к инфраструктуре кибершпионские группировки переходят к этапу закрепления для обеспечения незаметного присутствия в системе: создают скрытые каналы связи с серверами управления, настраивают сетевые туннели и внедряют инструменты, такие как ВПО для удаленного управления (59%).

Рисунок 12. Типы ВПО, использованного в атаках кибершпионских группировок на промышленные организации (доля успешных атак с использованием ВПО, 2024–2025)

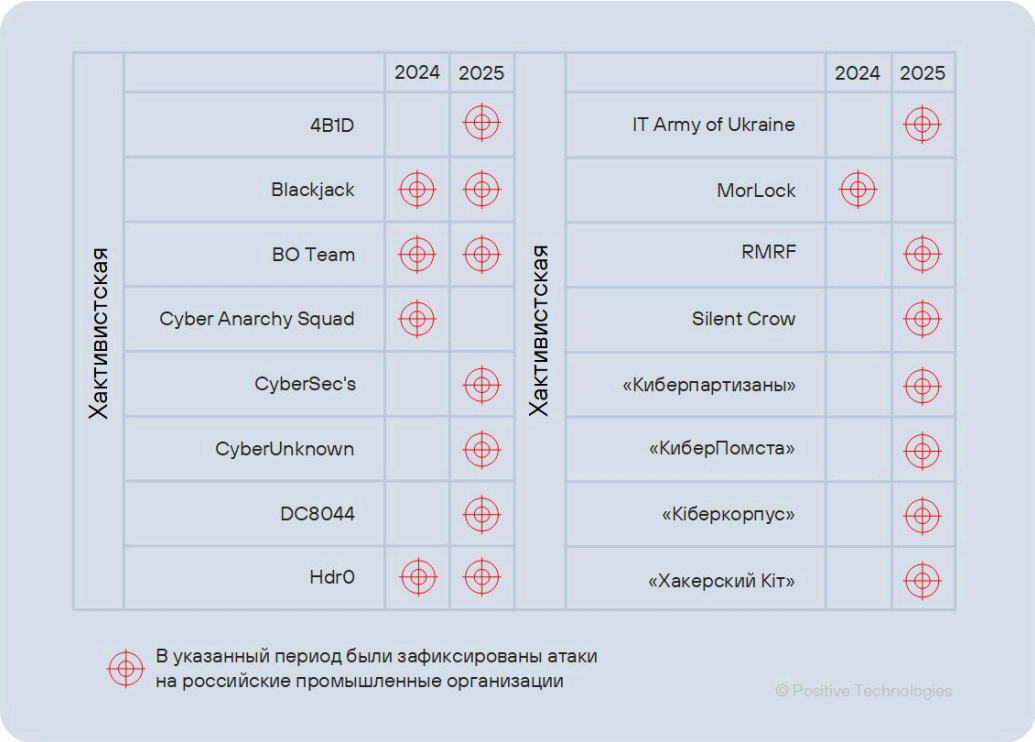
Большая часть кибершпионских групп широко применяет легитимные средства, которые не нужно загружать извне — они уже есть в скомпрометированной системе. Эту технику называют living off the land (LOL binaries, LOLBins). Использование таких инструментов позволяет минимизировать следы, маскируя активность под обычную работу администратора, снижая вероятность обнаружения.

Почти четверть (23%) рассматриваемых группировок использует инструменты, предназначенные для специалистов по информационной безопасности (red-team-фреймворки). Помимо уже ставшего классикой коммерческого ПО Cobalt Strike, злоумышленники активно внедряют в свой арсенал его альтернативные варианты с открытым исходным кодом — Sliver и Havoc. Например, так поступила уже упомянутая нами группировка QuietCrabs.

Хактивистские группировки

По нашим данным, более четверти кибератак (28%) против российских промышленных предприятий в 2024 и 2025 году совершили хактивисты. Мы наблюдали активность как минимум 16 таких групп.

Рисунок 13. Атаки хактивистских группировок на российские промышленные предприятия (2024–2025)



Хактивистские группировки преследуют преимущественно идеологические и политические цели. Классическими методами их воздействия обычно являются DDoS-атаки и дефейс — изменение главной страницы веб-ресурса, размещение на ней лозунгов, символики или агитационных материалов. В атаках на российские промышленные предприятия эти методы использовались, но реже: доля DDoS-атак на 18 п. п. ниже, чем в среднем по всем отраслям в России. В указанном случае другие методы являются более действенными инструментами давления.

Рисунок 14. Методы атак хактивистских группировок на промышленные предприятия и организации различных отраслей в России (доля успешных атак, 2024–2025)

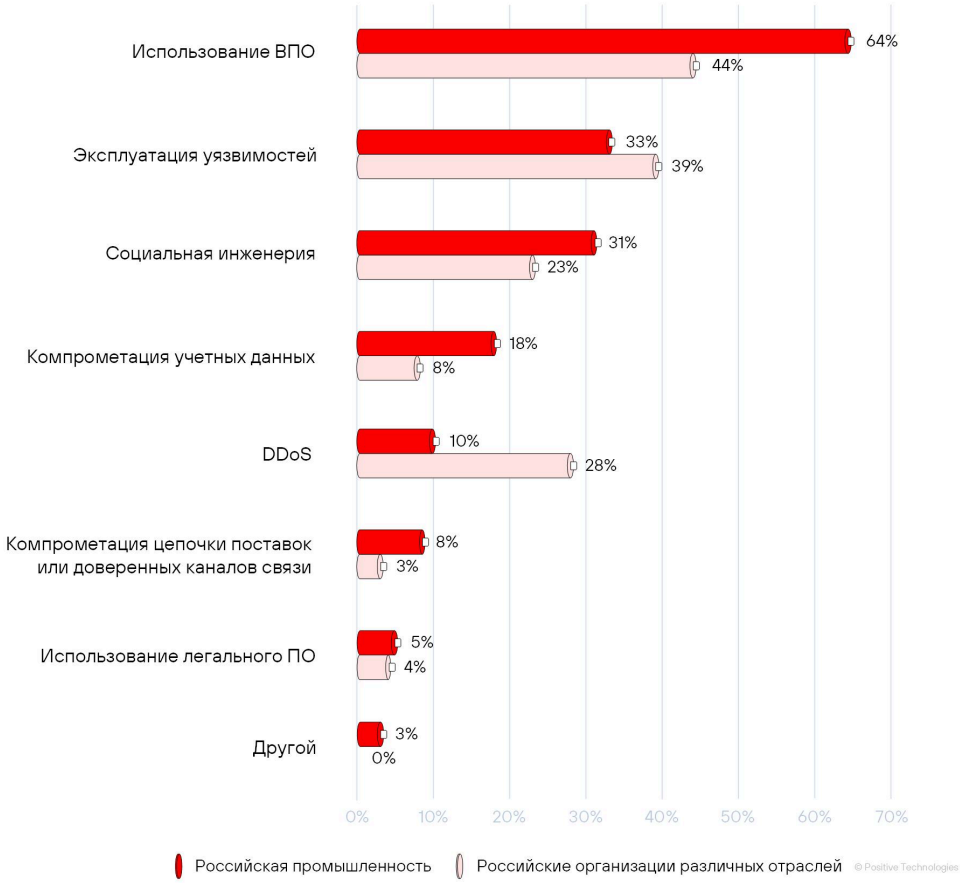
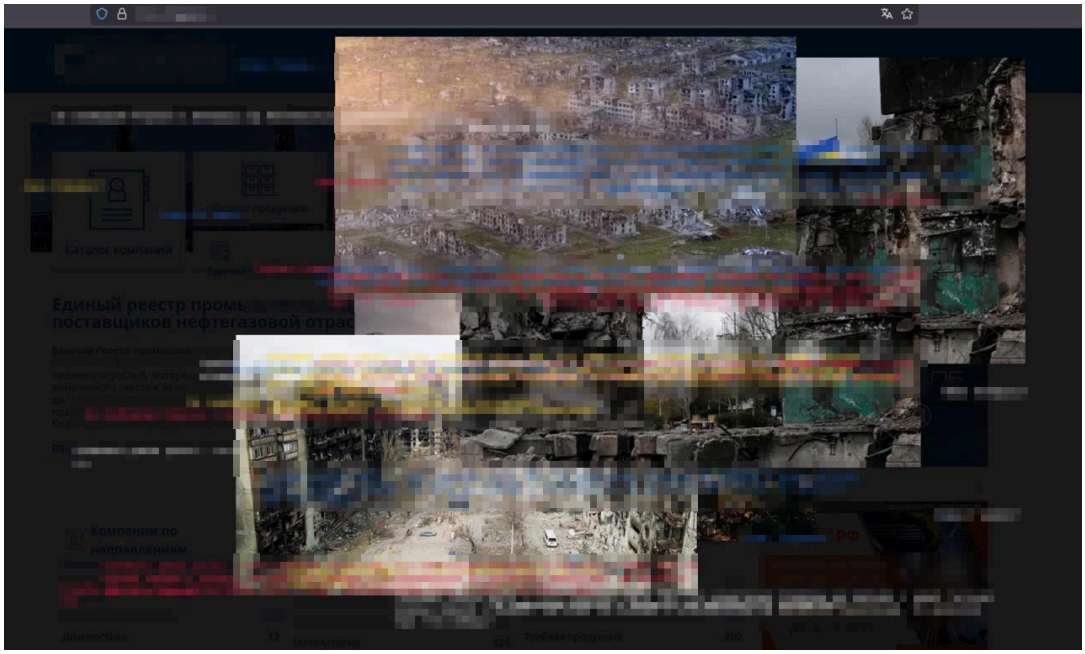
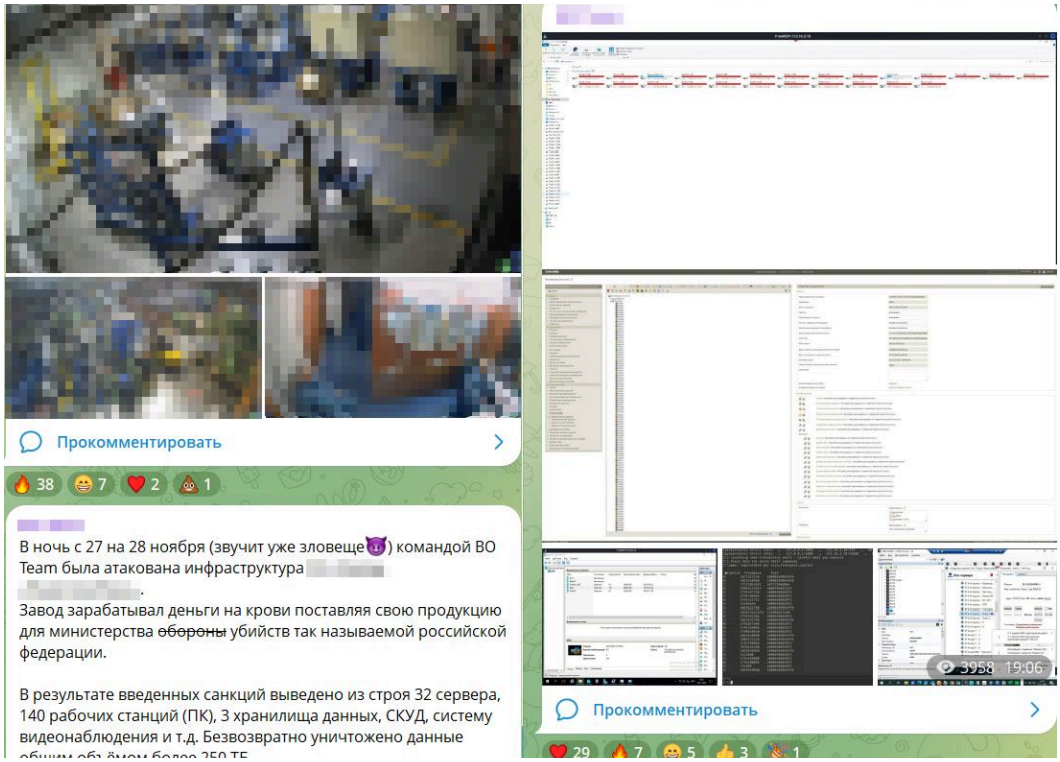


Рисунок 15. Пример дефейса сайта одной из российских промышленных компаний



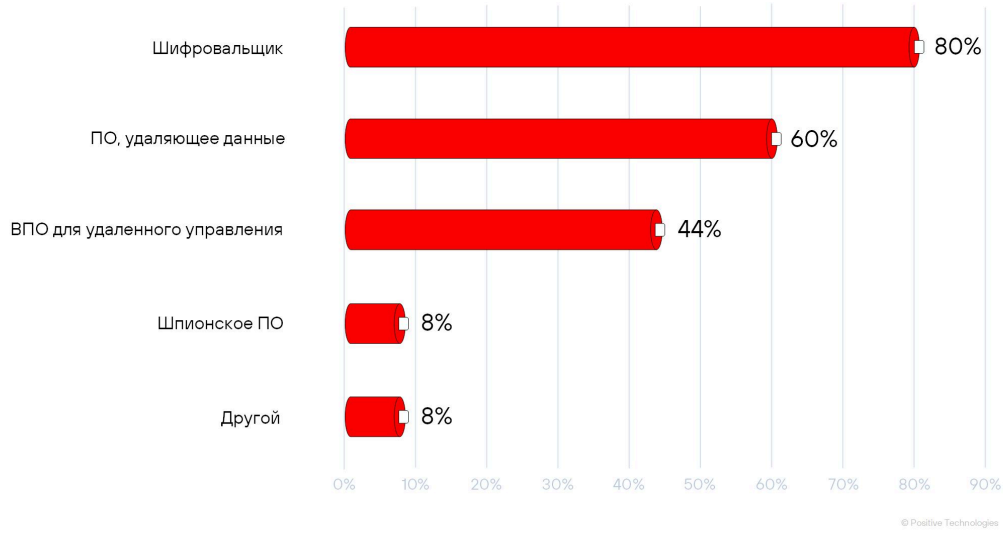
Главной целью хактивистских кибератак на промышленные предприятия в России было полное разрушение скомпрометированной инфраструктуры. По нашим данным, более чем три четверти (79%) инцидентов приводили к нарушению основной деятельности организации. Для хактивистов характерны демонстративность и ориентация на общественный резонанс, поэтому почти всегда информацию о своих «подвигах» они публикуют в личных Telegram-каналах или других социальных сетях.

Рисунок 16. Сообщение хактивистов с доказательствами взлома российского промышленного предприятия в конце 2025 года



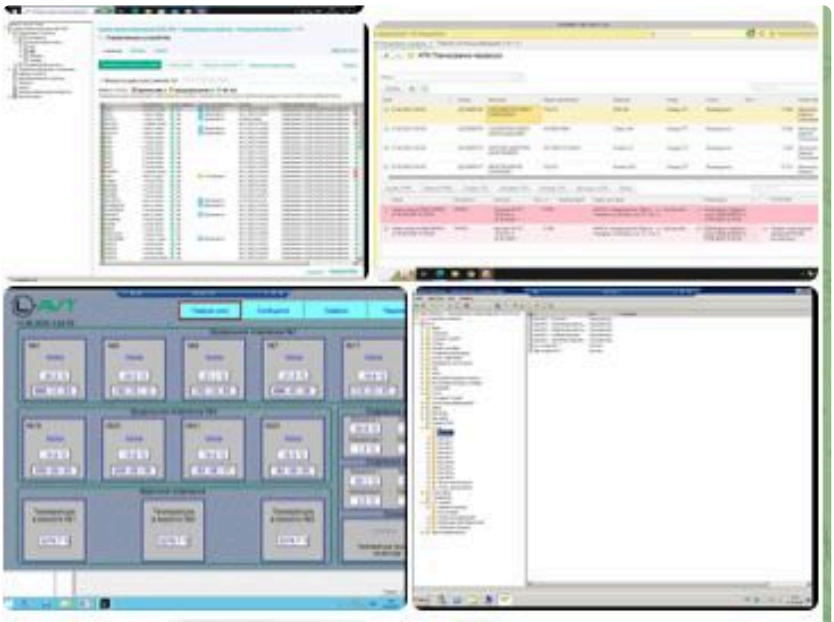
Для реализации разрушительных сценариев зачастую применяется вредоносное ПО (64%). Как правило, злоумышленники прибегают к использованию шифровальщиков (80% атак с применением ВПО). Преимущественно арсенал атакующих состоит из программ-вымогателей LockBit Black (3.0) и Babuk. Напомним, что билдер первого попал в публичное пространство в 2022 году, исходный код второго — в 2021-м, что во многом способствовало их распространению. Чуть реже группы прибегают к использованию ПО, удаляющего данные (60% атак с применением ВПО). Оно не оставляет жертве пространства для переговоров и служит исключительно для выведения систем из строя.

Рисунок 17. Типы ВПО, использованного в атаках хактивистов на промышленные организации (доля успешных атак с использованием ВПО, 2024–2025)



Нередко хактивисты прибегают к краже информации из инфраструктуры жертвы (41%): утечка данных создает большой инфоповод и позволяет дольше удерживать внимание аудитории. Так, более половины (52%) всех объявлений в дарквебе, связанных с утечками из отечественных промышленных организаций, представляют собой раздачу украденных данных. Например, в результате атаки группировки 4B1D на одного из производителей алкогольной продукции преступники сообщили о краже 700 ГБ данных, включая документацию, договоры, персональные данные и архивы переписки. В качестве подтверждения была опубликована ссылка на архив с данными.

Рисунок 18. Заявление хактивистов об атаке на российского производителя алкогольной продукции



Інцидент: [redacted]

Опис:
Підприємство повністю втратило контроль над ключовими елементами інфраструктури.

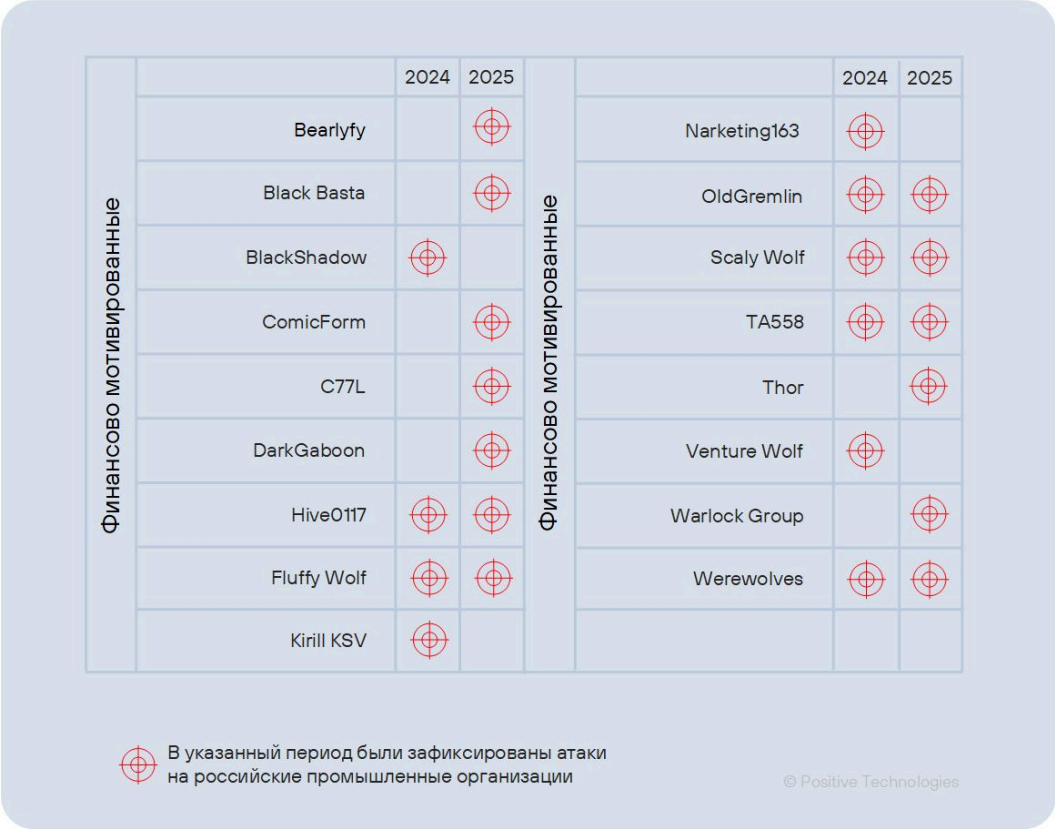
Що зроблено:

✅ Буквально знищено понад 300 комп'ютерів — техніка фізично виведена з ладу, відновленню не підлягає
✅ 16 серверів зашифровано, включно з контролерами домену, файлами логістики, бухгалтерії та обліку
✅ SCADA-система — зашифрована, керування втрачене
✅ Повне шифрування критичних бізнес-процесів
✅ Вивантажено понад 700 ГБ даних: документація, договори, технологічні карти,

Финансово мотивированные группировки

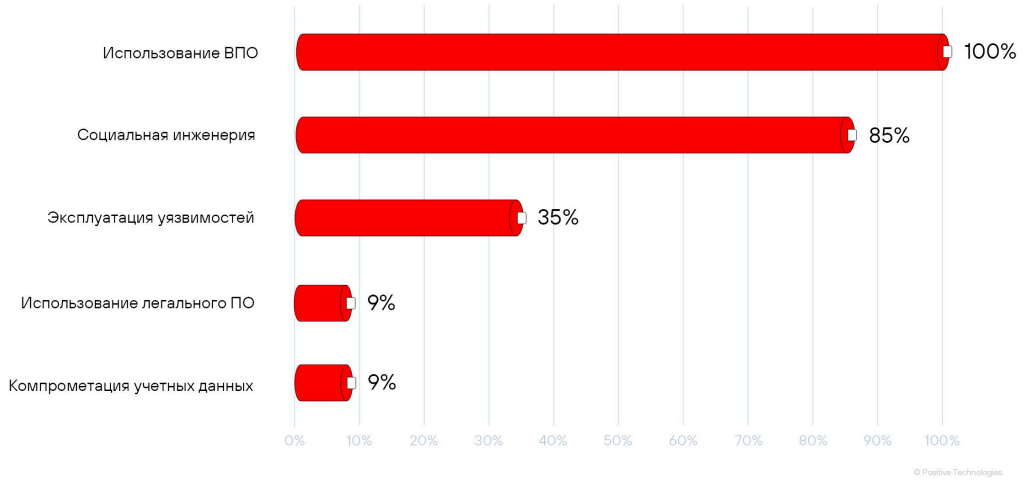
Часть злоумышленников (25%), атакующих российские промышленные предприятия, преследовали цель, связанную с получением финансовой выгоды. На протяжении рассматриваемого периода были активны как минимум 17 таких группировок.

Рисунок 19. Атаки финансово мотивированных группировок на российские промышленные предприятия (2024–2025)



Нередко финансово мотивированные злоумышленники совершают атаки без привязки к стране или отрасли: например, создают фишинговые рассылки, нацеленные сразу на множество организаций. В исследовании рассматривались только преступные группировки, жертвами которых становились промышленные организации, поэтому фактическое число финансово мотивированных групп, атаки которых затронули сектор, может быть выше. Целью этих атакующих является быстрый и измеримый результат: получение выкупа, кража или монетизация данных. Для реализации планов им необходим инструмент — вредоносное ПО, которое применялось в каждом киберинциденте (100%).

Рисунок 20. Методы атак финансово мотивированных группировок на промышленные предприятия (доля успешных атак, 2024–2025)



В качестве орудия киберпреступлений группировки чаще всего отдавали предпочтение ВПО для удаленного управления (62%). Оно позволяет установить полный контроль над инфраструктурой жертвы и подготовить почву для монетизации атаки: переместиться по сети, найти ценные данные и определить ключевые активы. Так, комбинация ВПО для удаленного управления и шифровальщика может позволить ограничить работу тех ресурсов, остановка которых причинит максимальный ущерб. В контексте атак на производственный сектор — злоумышленники могут найти забытый сетевой маршрут до технологической сети и зашифровать все АРМ инженеров и операторов, SCADA-серверы. Действия нарушителей могут привести к потере возможности управлять технологическим процессом или к его полной остановке. Эти события являются недопустимыми для промышленного предприятия, из-за чего преступники полагают, что компания охотнее согласится на выкуп.

Рисунок 21. Типы ВПО, использованного в атаках финансово мотивированных группировок на промышленные организации (доля успешных атак с использованием ВПО, 2024–2025)

Кроме того, в ВПО для удаленного управления нередко внедряются функции, характерные для вредоносов других типов, в частности — для шпионского ПО. Это позволяет финансово мотивированным атакующим достичь для них приоритетной цели — украсть информацию.

Рисунок 22. Фишинговая счет-фактура, которую группировка OldGremlin использовала для доставки шпионского ПО XWorm (источник: PT ESC)

Счет-фактура № 23891-2 от "09" Августа 2024г. (1)
Исправление № — от — (1а)

Приложение № 1 к постановлению Правительства Российской Федерации от 26 декабря 2011 г. № 1137 (в редакции постановления Правительства Российской Федерации от 2 апреля 2021 г. № 534)

Продавец	ООО [redacted] (2)	**Покупатель**	(6)
Адрес	129090, город Москва, [redacted] (2а)	Адрес	(6а)
ИНН/КПП продавца	[redacted] (2б)	ИНН/КПП покупателя	(6б)
Грузоотправитель и его адрес	— (3)	Валюта: наименование, код	Российский рубль, 643 (7)
Грузополучатель и его адрес	— (4)	Идентификатор государственного контракта, договора (соглашения) (при наличии)	(8)
К платежно-расчетному документу	№ 23891-2 от 01.08.2024 (5)		
Документ об отгрузке	— (5а)		

№ п/п	Наименование товара (описание выполненных работ, оказанных услуг), имущественного права	Код вида товара	Единица измерения: код	Единица измерения: условное обозначение (национальное)	Количество (объем)	Цена (тариф) за единицу измерения	Стоимость товаров (работ, услуг), имущественных прав без налога - всего	В том числе сумма акциза	Налоговая ставка	Сумма налога, предъявляемая покупателю	Стоимость товаров (работ, услуг), имущественных прав с налогом - всего	Страна происхождения товара: цифровой код	Страна происхождения товара: краткое наименование	Регистрационный номер декларации на товары или регистрационный номер партии товара, подлежащего прослеживаемости	Количественная единица измерения товара, используемая в целях прослеживаемости: код	Количественная единица измерения товара, используемая в целях прослеживаемости: условное обозначение	Количество товара, подлежащего прослеживаемости, в количественной единице измерения товара
1	1а	1б	2	2а	3	4	5	6	7	8	9	10	10а	11	12	12а	13
1	Консультационные услуги в сфере маркетинга	—	—	—	—	—	—	—	20/120	250 000,00	1 500 000,00	—	—	—	—	—	—
Итого							1 250 000,00	X		250 000,00	1 500 000,00						
Всего к оплате							1 250 000,00	X		250 000,00	**1 500 000,00**						

Руководитель организации или иное уполномоченное лицо [redacted] (подпись) [redacted] (Ф.И.О.)

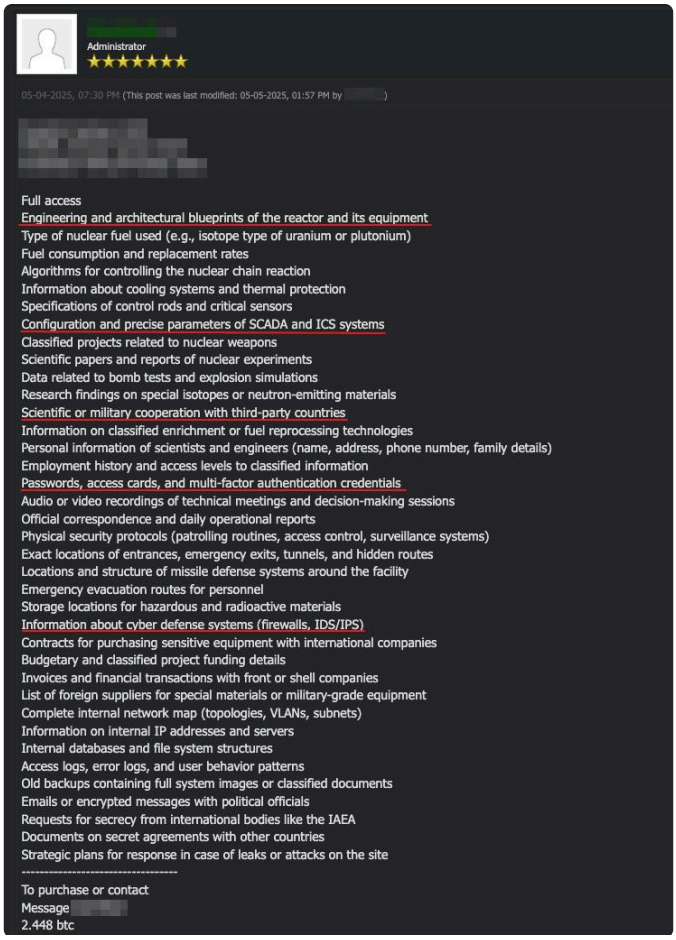
Главный бухгалтер или иное уполномоченное лицо [redacted] (подпись) [redacted] (Ф.И.О.)

Индивидуальный предприниматель или иное уполномоченное лицо [redacted] (подпись) [redacted] (Ф.И.О.) [redacted] (реквизиты свидетельства о государственной регистрации индивидуального предпринимателя)

Шифровальщики применялись более чем в трети (35%) кибератак финансово мотивированных злоумышленников. В их инвентаре, как и у хактивистов, встречаются LockBit Black (3.0), Babuk. Некоторые злоумышленники являются участниками партнерских программ — используют вредоносы, распространяемые по модели RaaS (ransomware as a service). Например, с марта 2025 года участники программы C77L совершили не менее 40 кибератак на российские и белорусские организации, в том числе из сферы производства.

Как мы отмечали ранее, одна из целей финансово мотивированных атакующих — кража конфиденциальной информации: более половины (59%) инцидентов заканчивались утечками. Часть этих кампаний связана с двойным вымогательством. Злоумышленники прекрасно понимают ценность похищенных данных и уверены, что, даже если компания не заплатит выкуп, их можно будет продать в дарквебе. Так, самая высокая заявленная стоимость набора информации, связанной с российским промышленным сектором, достигала около 300 тыс. долларов (2,488 BTC). По утверждению продавца, в архиве содержались отчеты экспериментов, персональные данные, учетные записи с паролями, протоколы совещаний, внутренние отчеты, финансовая документация, схемы охраны, планы расположения объектов, эвакуационные маршруты и другая информация.

Рисунок 23. Объявление о продаже данных, похищенных из российской промышленной организации



Атаки на технологический сегмент

Сеть промышленного предприятия представляет собой многоуровневую инфраструктуру, объединяющую корпоративный и технологический сегмент. Обычно сегменты разделяет воздушный зазор.

Рисунок 24. Упрощенная схема сети промышленной организации

Корпоративная сеть (ИТ-сегмент) состоит из офисных рабочих станций, почтовых и файловых серверов, систем класса ERP и CRM[8] и других бизнес-приложений.

Технологический сегмент (ОТ), как правило, подразделяется на три уровня. На верхнем располагается SCADA-система, автоматизированные рабочие места (АРМ) операторов, инженеров и начальника производства. Как правило, на этих устройствах поверх классических ОС — Windows и Linux — установлено специализированное ПО, необходимое для осуществления технологического процесса. Значит, большая часть техник злоумышленников, используемых в атаках на корпоративный сегмент, применимы и к верхнему уровню технологической сети.

Сервер SCADA обычно имеет два сетевых интерфейса: один для подключения с узлов верхнего уровня (например, с АРМ инженеров), второй — для коммуникации с программируемыми логическими контроллерами (ПЛК). В ПЛК закладывается логика технологических процессов: именно контроллеры взаимодействуют с реальными датчиками и исполнительными механизмами и могут оказывать влияние на их работу. Между ПЛК и SCADA-системой идет активный обмен информацией. ПЛК сообщает SCADA-системе о значениях параметров технологического процесса, а та в свою очередь визуализирует параметры в понятном для оператора виде. Это работает и в другую сторону: SCADA-система, получив команду от оператора или выполнив заложенный в проект алгоритм, отправляет на ПЛК специализированные команды, которые переключают режимы работы оборудования, — тем самым она осуществляет регулирование технологического процесса.

На нижнем уровне технологической сети располагаются датчики (например, давления или температуры) и исполнительные устройства (двигатели, заслонки).

Атаки на технологический сегмент происходят реже, чем на ИТ-сегмент, однако они приводят к критическому урону: даже одно неавторизованное вмешательство может остановить производство, нарушить процессы, вывести из строя оборудование и даже спровоцировать катастрофу. Кроме того, для обеспечения безопасности корпоративного сегмента существует широкий спектр развитых решений — от EPP и EDR-систем до продуктов класса SIEM. В то же время для технологического сегмента выбор инструментов существенно ограничен: требуются специализированные решения, совместимые с промышленным оборудованием и учитывающие особенности производственных процессов.

[8] ERP- и CRM-системы — программные системы для автоматизации бизнеса. Продукты класса CRM помогают выстраивать работу с клиентами, ERP-решения — управлять внутренними ресурсами.

Подробное описание инцидентов, затрагивающих технологический сегмент, крайне редко становится публичным. Это связано не только с репутационными рисками, но и с тем, что оно может содержать сведения о конфигурации производственных систем, мерах защиты и другую информацию, актуальность которой сохраняется длительное время: инфраструктура промышленного сегмента обновляется крайне редко. В итоге сведения о таких инцидентах, как правило, остаются у ограниченного круга специалистов.

Тем не менее для построения эффективной стратегии защиты необходимо понимать, как действуют атакующие. Поэтому рассмотрим наиболее распространенные угрозы для технологического сегмента на примере отчетов с нескольких кибербитв Standoff — соревнований, на которых специалисты по ИБ проверяют свои навыки. На мероприятии используются настоящие промышленные контроллеры и АСУ ТП — условия максимально приближены к реальным. Кроме того, совместно с командой PT ISIM мы подготовили рекомендации по обнаружению описываемых атак и реагированию на них.

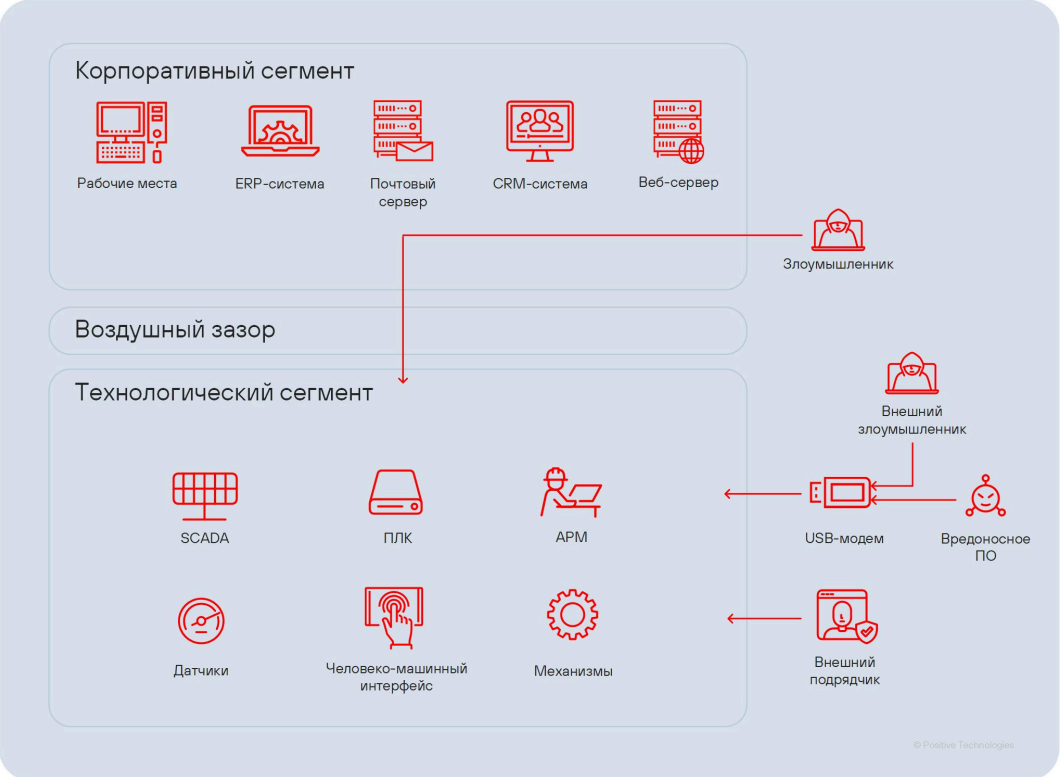
Цель красных команд на соревнованиях Standoff — реализовать недопустимое событие, в результате которого становится невозможным достижение операционных и стратегических целей организации или которое приводит к длительному нарушению ее основной деятельности. Например, таким событием может быть остановка работы паровой турбины, кража средств со счетов в банках, сход поезда с рельсов.

Как злоумышленники попадают в технологический сегмент

Многое из того, что мы описали ранее, относится к атакам на корпоративный сегмент инфраструктуры промышленных организаций. Как мы отметили, он должен быть изолирован от технологического, однако на практике для решения рабочих задач часто оставляют возможность сетевой коммуникации между ними. В результате, блуждая по корпоративной инфраструктуре, злоумышленник, возможно сам того не понимая, может оказаться в технологическом сегменте сети. Так, по данным Zero Networks, 75% атак на OT начинаются с компрометации ИТ-инфраструктуры.

Ярким подтвержденным примером подобной кибератаки является инцидент, произошедший на немецком металлургическом заводе в 2014 году. Злоумышленники получили первоначальный доступ к офисной сети при помощи социальной инженерии и далее переместились в производственный сегмент организации. В результате их действий компоненты системы управления и производственные машины вышли из строя. Сбои помешали заводу должным образом остановить доменную печь, из-за чего произошли масштабные повреждения всей всей инфраструктуры.

Рисунок 25. Упрощенная схема получения доступа к технологическому сегменту злоумышленниками



Один из способов получения доступа к OT из ИТ-сегмента — подключение по протоколам удаленного доступа (RDP и SSH) к SCADA-серверу. Использование протокола RDP фиксировалось во всех рассмотренных нами отчетах с кибербитв Standoff.

Угроза: нарушение безопасности периметра технологической сети

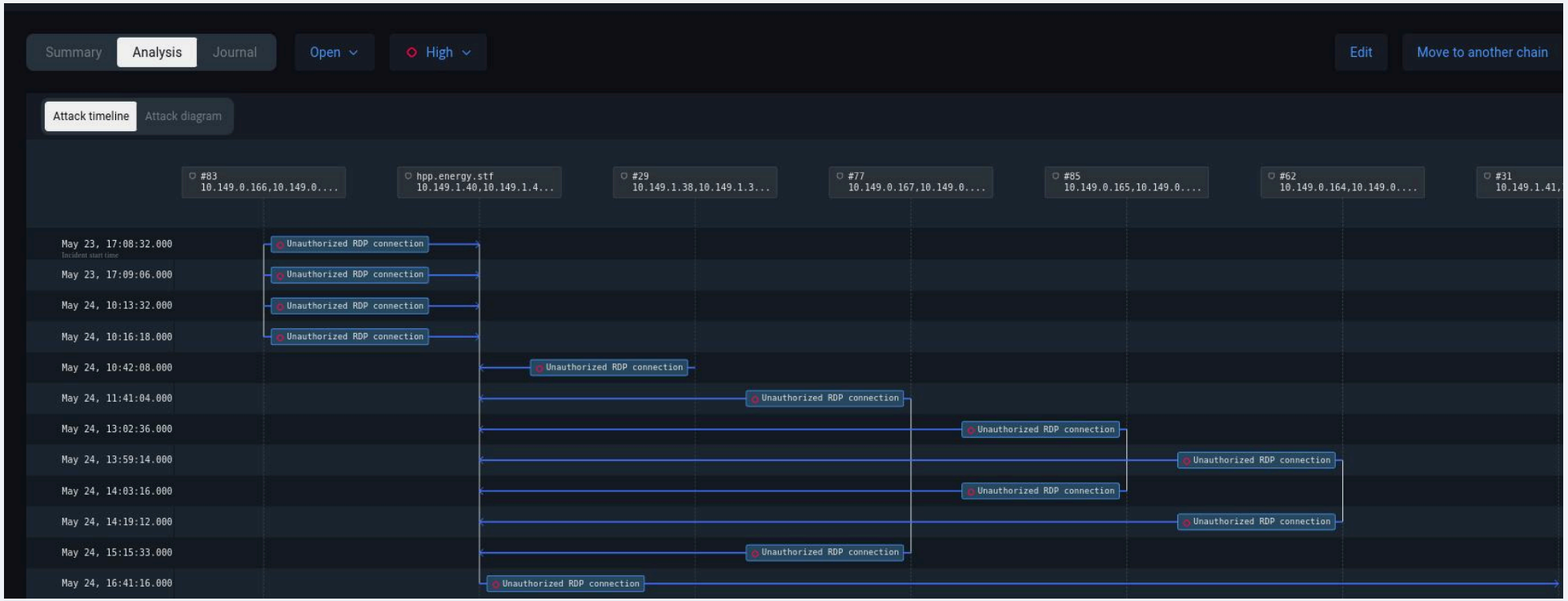
Как отслеживать такие события и реагировать на них

Нарушения ИБ периметра технологической сети можно выявить посредством анализа трафика между ИТ- и OT-сегментом: удаленный доступ сопровождается активностью по таким протоколам, как RDP и SSH.

Очевидный признак инцидента — появление соединений между ранее не взаимодействовавшими узлами. Чтобы отслеживать эти события, система обеспечения информационной безопасности (СОИБ) должна фиксировать легитимные соединения и сигнализировать о появлении новых. При их обнаружении необходимо уточнить у специалистов, обслуживающих АСУ ТП, является ли коммуникация штатной: она может быть связана с изменениями в инфраструктуре.

В более сложных случаях, например при компрометации учетных данных администратора, регулярно подключающегося из корпоративной сети к АРМ по протоколу удаленного доступа, для выявления атак требуется анализировать поведение пользователя.

Рисунок 26. Пример обнаружения продуктом PT ISIM подключения по RDP



Существуют и другие способы перехода злоумышленников из ИТ-сегмента в технологический. Об одном из них подробно рассказал анонимный участник кибербитвы Standoff в статье для журнала Positive Research. Команда обнаружила учетную запись, позволяющую выполнить атаку DCSync[9]. С ее помощью участники получили данные администратора и сделали дамп всех учетных записей в домене. Далее через групповые политики (GPO) команда создала задание на установку соединения с C2-сервером и получила доступ ко всем компьютерам в домене.

Угроза: нарушение безопасности периметра технологической сети

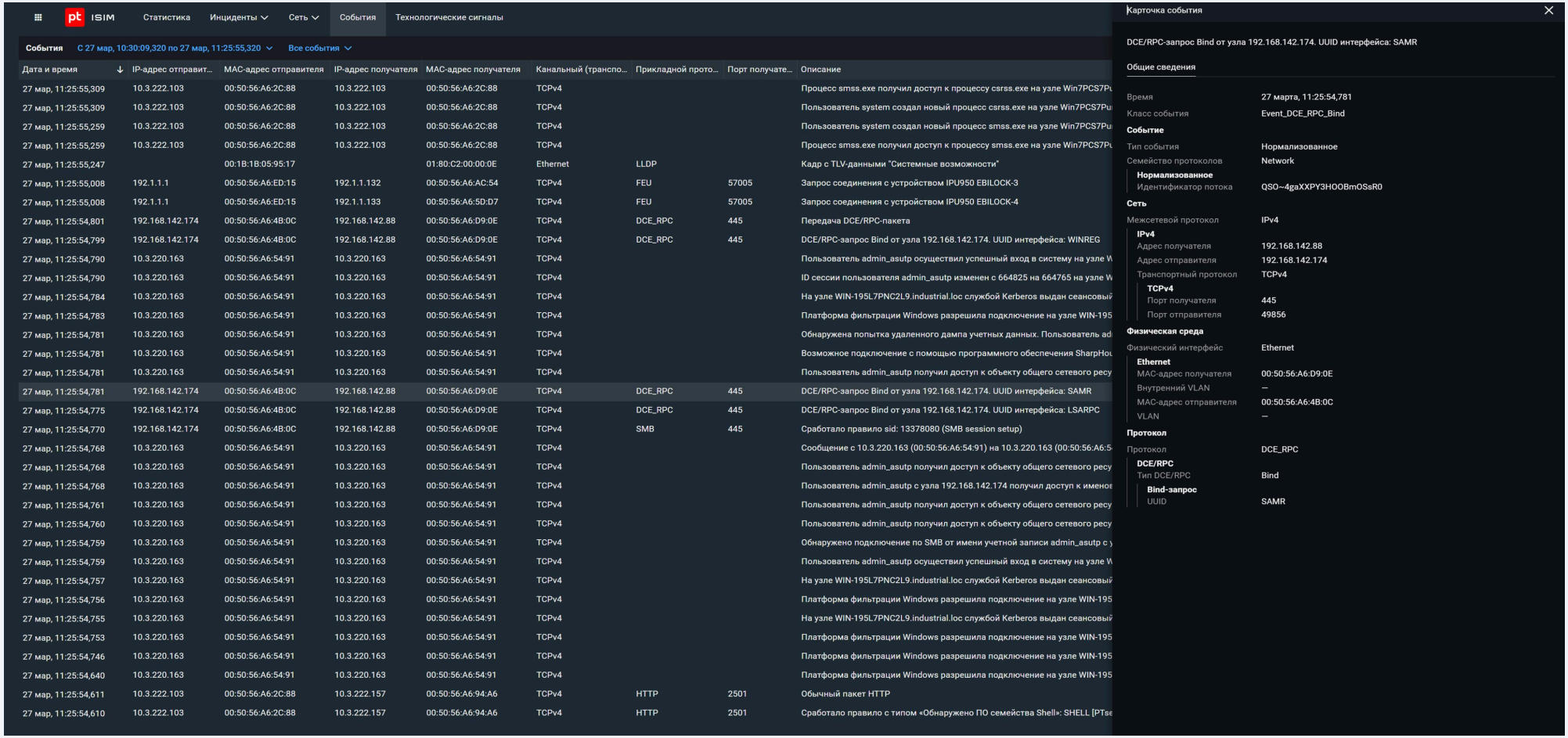
В описанном примере нарушение ИБ периметра технологической сети происходило в несколько этапов. Рассмотрим, к*ак отслеживать эти шаги по отдельности и реагировать на них*.

Шаг 1. Проведение атаки DCSync. Первым шагом в рассматриваемом сценарии является получение учетных данных, а именно — реализация атаки DCSync. Для ее обнаружения необходимо вести мониторинг журнала событий на контроллере домена, анализировать его на предмет запросов, связанных с репликацией, и других действий, которые могут осуществляться в рамках DCSync. Необходимо отслеживать сетевую активность контроллеров домена: анализировать соединения по протоколу DCE/RPC[10], искать запросы, свидетельствующие о начале репликации со стороны узла, который не является контроллером домена, или о ее аномалиях.

[9] DCSync — атака, позволяющая злоумышленнику выдать себя за контроллер домена с целью получения учетных данных пользователей.

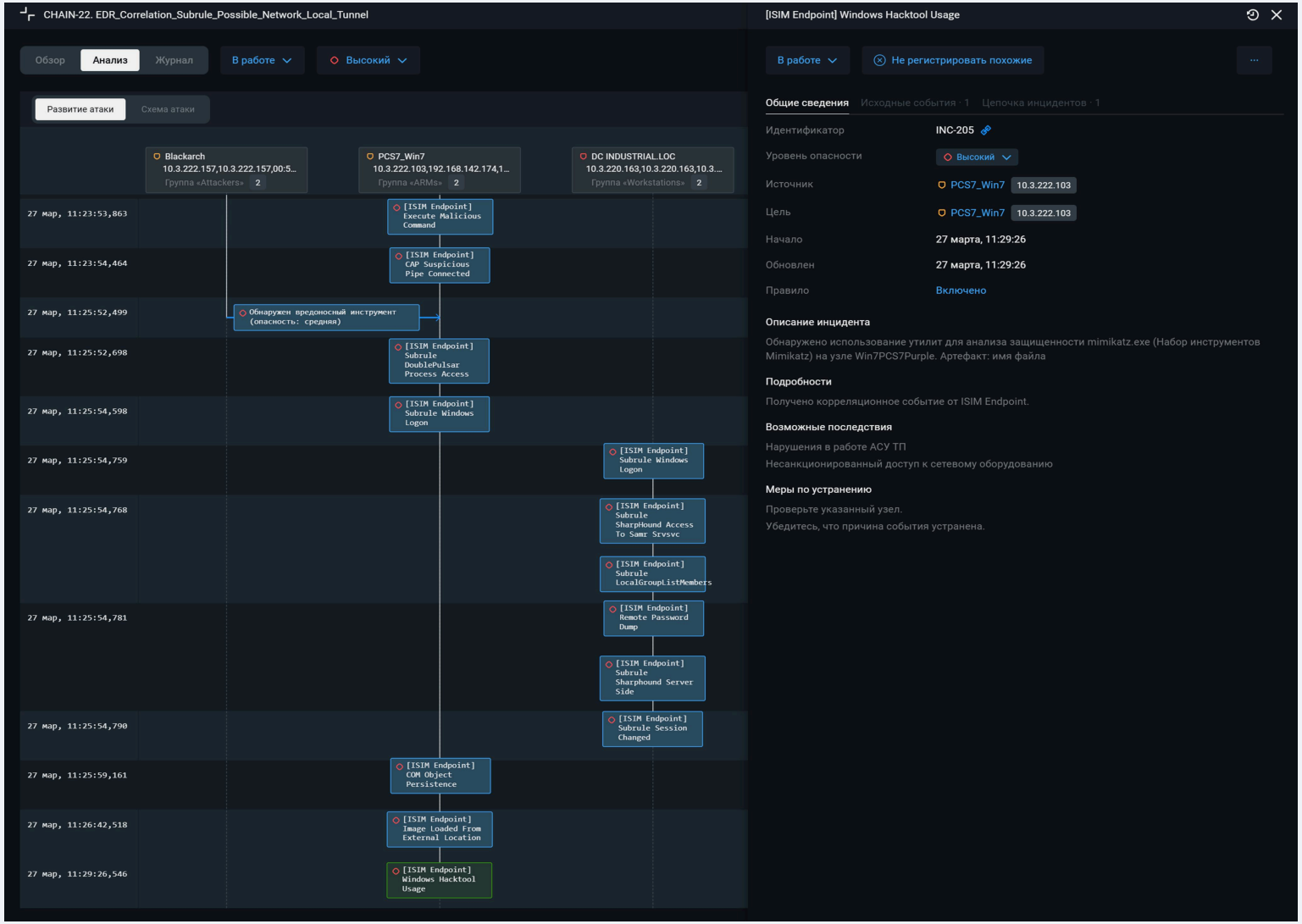
[10] DCE/RPC (Distributed Computing Environment/Remote Procedure Call) — стандарт протокола удаленного вызова процедур, который обеспечивает взаимодействие между клиентскими и серверными приложениями в удаленных системах.

Рисунок 27. Пример обнаружения соединения по протоколу DCE/RPC при помощи PT ISIM



Необходимо детектировать события запуска утилит, позволяющих провести атаку DCSync, например Mimikatz или *secretsdump.py*.

Рисунок 28. Пример обнаружения продуктом PT ISIM использования утилиты Mimikatz



Шаг 2. Изменение групповых политик. Необходимо отслеживать события, связанные с добавлением пользователей в группы безопасности, и фиксировать изменение или создание объектов Active Directory в журналах безопасности на контроллерах домена.

Рисунок 29. Пример обнаружения продуктом PT ISIM создания групповой политики

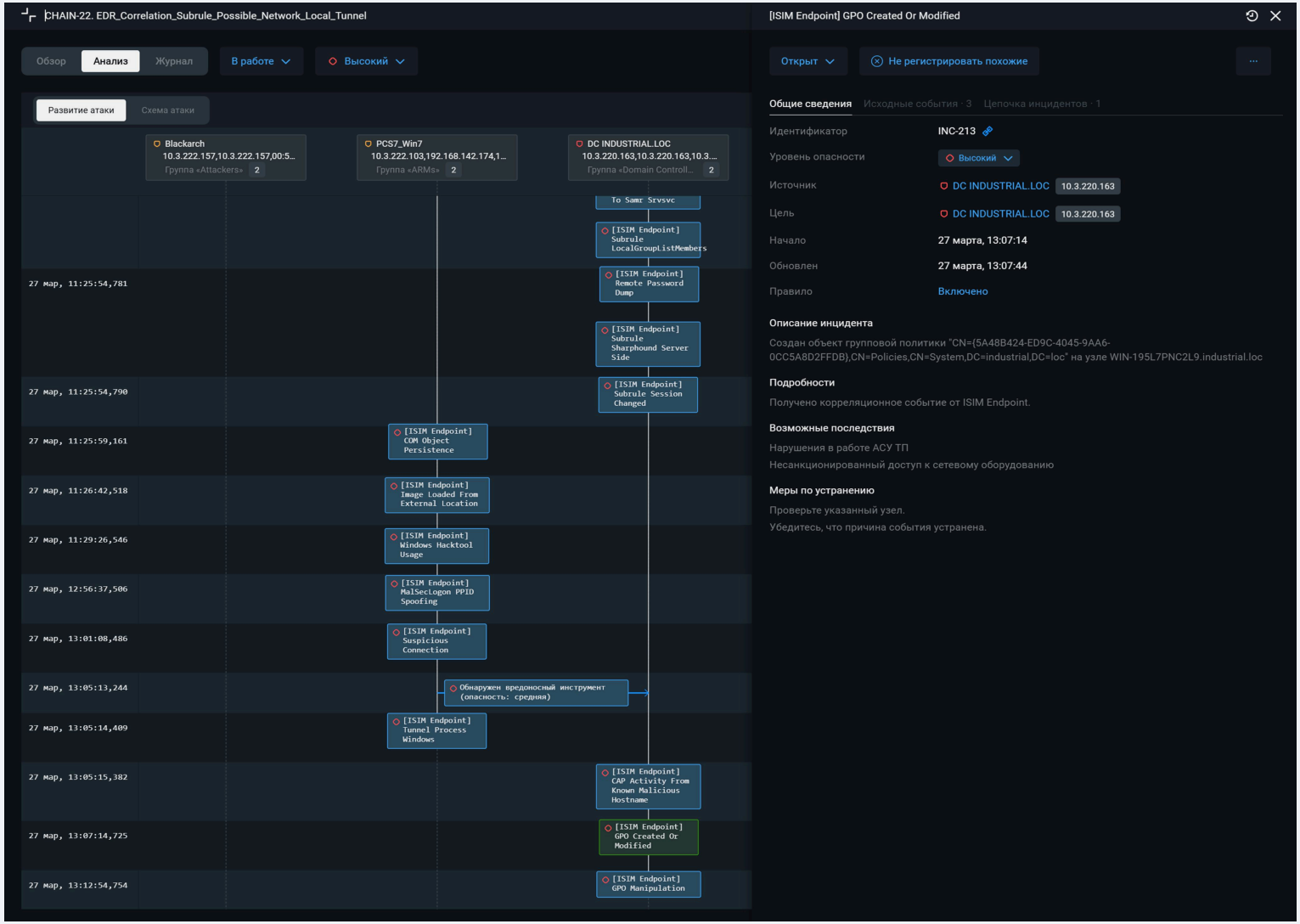
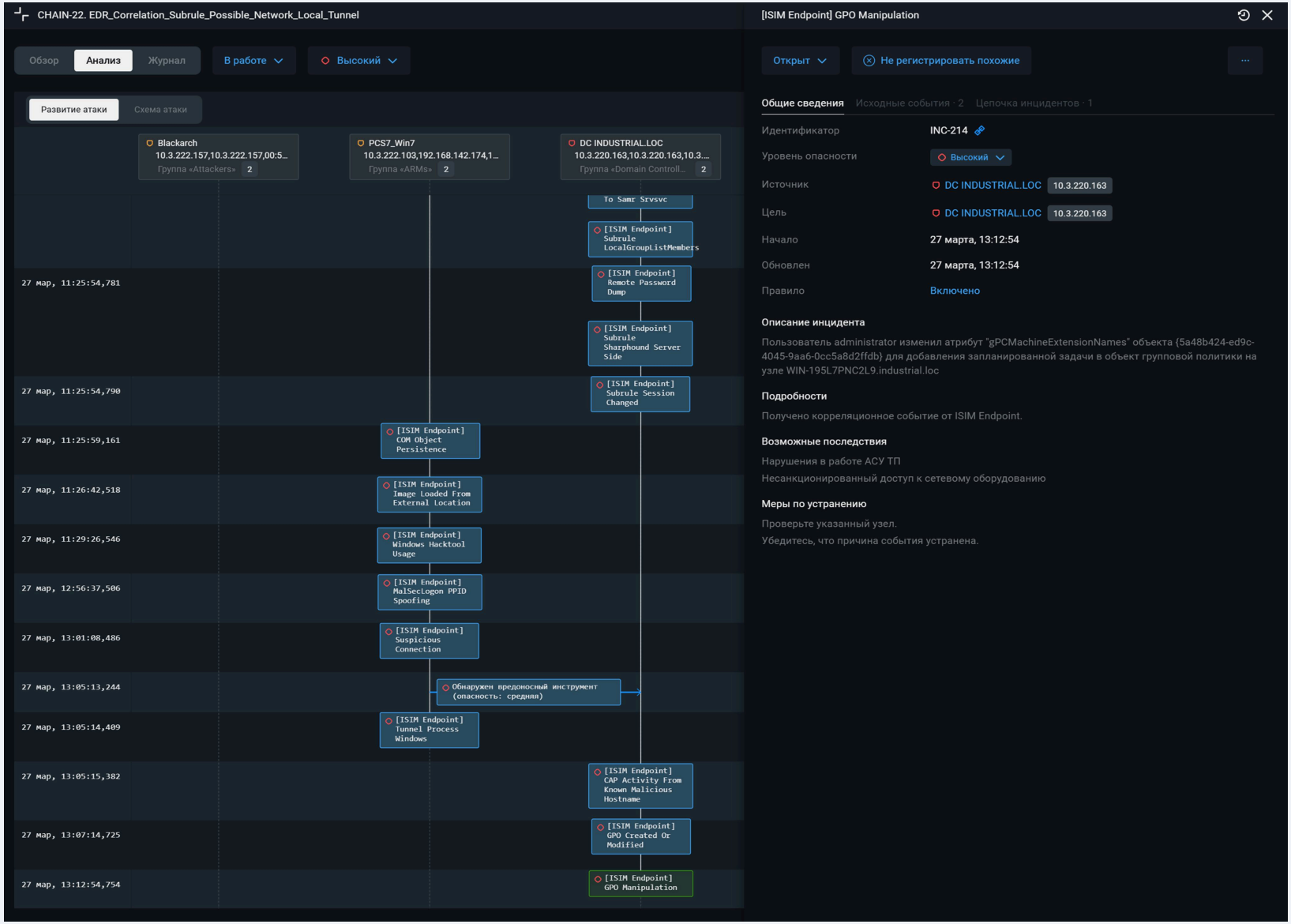


Рисунок 30. Пример обнаружения продуктом PT ISIM изменения групповой политики



При реагировании на описанный сценарий необходимо:

- Отозвать привилегии у скомпрометированной учетной записи.
- Заблокировать учетную запись и сменить пароли на всех учетных записях.
- Удалить вредоносные GPO-задачи.
- Остановить подозрительные процессы, закрыть или заблокировать подозрительные сетевые соединения.

Кибератака может начаться и из самого изолированного технологического сегмента. В этом случае играет роль человеческий фактор. Например, даже при наличии формальных ограничений оператор может подключить к АРМ зараженное запоминающее USB-устройство.

Угроза: нарушение безопасности периметра технологической сети

Как отслеживать такие события и реагировать на них

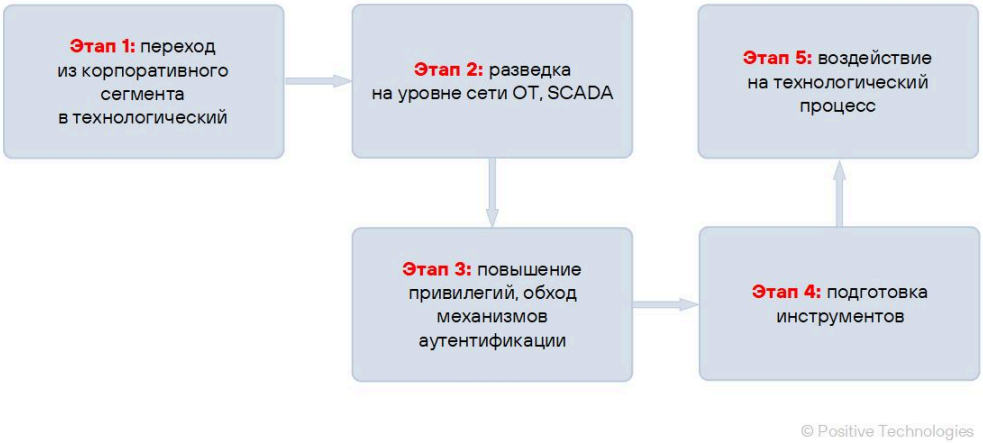
Обнаруживать такие нарушения лучше с помощью средств защиты конечных устройств, которые могут не только предупредить оператора, но и заблокировать подключение.

Еще один вектор проникновения в технологический сегмент — компрометация инфраструктуры подрядчика, обслуживающего и поддерживающего технологическое оборудование и имеющего удаленный доступ к промышленной сети. В этом случае компрометация происходит через легитимные механизмы, что затрудняет своевременное обнаружение угрозы. Для выявления инцидента также требуется анализ поведения пользователя.

Как злоумышленники действуют в технологическом сегменте

После получения доступа к технологическому сегменту (этап 1) действия злоумышленников можно разделить на 4 основных шага. Рассмотрим каждый из них более подробно.

Рисунок 31. Основные этапы атаки на технологический сегмент сети на соревнованиях Standoff



Этап 2: разведка на уровне сети OT, SCADA

Получив доступ к технологической сети предприятия, злоумышленники изучают структуру системы управления: контроллеры, SCADA-серверы, технологические протоколы и логику производственного процесса. Этот шаг необходим, чтобы понять, как именно можно повлиять на оборудование для достижения своих целей.

Недопустимое событие «Остановка очистки нефти в электродегидраторе на нефтеперерабатывающем заводе». Получив первоначальный доступ к инфраструктуре, команда просканировала порт 102 — он используется для работы протокола ISO-on-TCP, который применяется в промышленных системах автоматизации (АСУ ТП), в частности в оборудовании Siemens. Так «красные» нашли ПЛК Siemens, после чего продолжили развивать атаку.

Обнаружив контроллер, злоумышленники могут попытаться использовать уязвимости в нем, чтобы:

- получить возможность выполнять привилегированные операции без авторизации либо с авторизацией, которую легко обойти;
- вызвать отказ в работе устройства при помощи недокументированных команд;
- добиться отказа в работе устройства при помощи обращения к несуществующим портам.

Угроза: атаки на ПЛК

Как отслеживать такие события и реагировать на них

Многие производители ПЛК ответственно подходят к устранению уязвимостей: публикуют бюллетени безопасности, выпускают обновления прошивки. Помощь им оказывают и исследователи из компаний, создающих продукты для защиты технологических сетей. Например, эксперты Positive Technologies обнаружили шесть уязвимостей в продукте CENTUM VP компании Yokogawa, решения которой широко применяются в отечественном производстве. Уязвимый код использовался как на серверах управления, так и в программируемых логических контроллерах, входящих в состав системы.

Для отслеживания попыток подобных атак необходимо, чтобы в СОИБ были заложены правила и индикаторы обнаружения угроз.

Этап 3: повышение привилегий, обход механизмов аутентификации

Чтобы осуществить вредоносные действия, у атакующих не всегда есть необходимые права оператора или администратора. Как следствие, злоумышленники могут использовать различные способы повышения привилегий или обхода механизмов аутентификации. Рассмотрим несколько примеров.

Недопустимое событие «Отключение уличного освещения». Атакующие обнаружили пароль оператора в папке проекта и использовали его для входа в SCADA-систему.

Недопустимое событие «Остановка работы комбината. Авария на прокатном станке: разрыв заготовки». Красная команда открыла интерфейс SCADA-системы и в настройках отключила аутентификацию.

Недопустимое событие «Остановка работы комбината. Пролив металла из сталеразливочного ковша МНЛЗ в цех». Команда заменила в конфигурационном файле *C:\wincc_oa_proj\ccm\config\progs* поле *auth "Creator" "some_hash"* на *auth "" ""* для сброса авторизации.

Недопустимое событие «Прекращение подачи электричества. Остановка работы гидроагрегата на гидроэлектростанции». Система SCADA запускается в приложении InTouch View, предназначенном для отображения графического интерфейса, визуализации технологических процессов и управления ими в реальном времени. Первоначально у красной команды нет необходимых прав, ей недоступны никакие действия. Атакующие закрыли приложение и в папке *C:\Users\Public\Documents\SCADA\HPP* поменяли название файла *password.bin* на *password.bin.bak*. После перезапуска SCADA-системы это изменение привело к сбросу логина и пароля до стандартных *administrator:wonderware*.

Файл проекта — сердце любой SCADA-системы. Изменить ее поведение зачастую можно просто подменив этот файл и перезапустив сервисы.

Недопустимое событие «Нарушение водоснабжения и водоотведения. Нарушение работы сооружений для очистки сточных вод». Атакующие создали проект *temp.hmi* для SCADA-системы. Файл *water_treatment_hmi\objects\LoginForm.omobj* заменили на свой, в созданный проект импортировали объекты из оригинального (*water_treatment_hmi\objects*), после чего собрали и запустили его. Таким образом, модификация файла проекта позволила команде добиться обхода авторизации.

Угроза: подмена файла проекта в системах SCADA и HMI

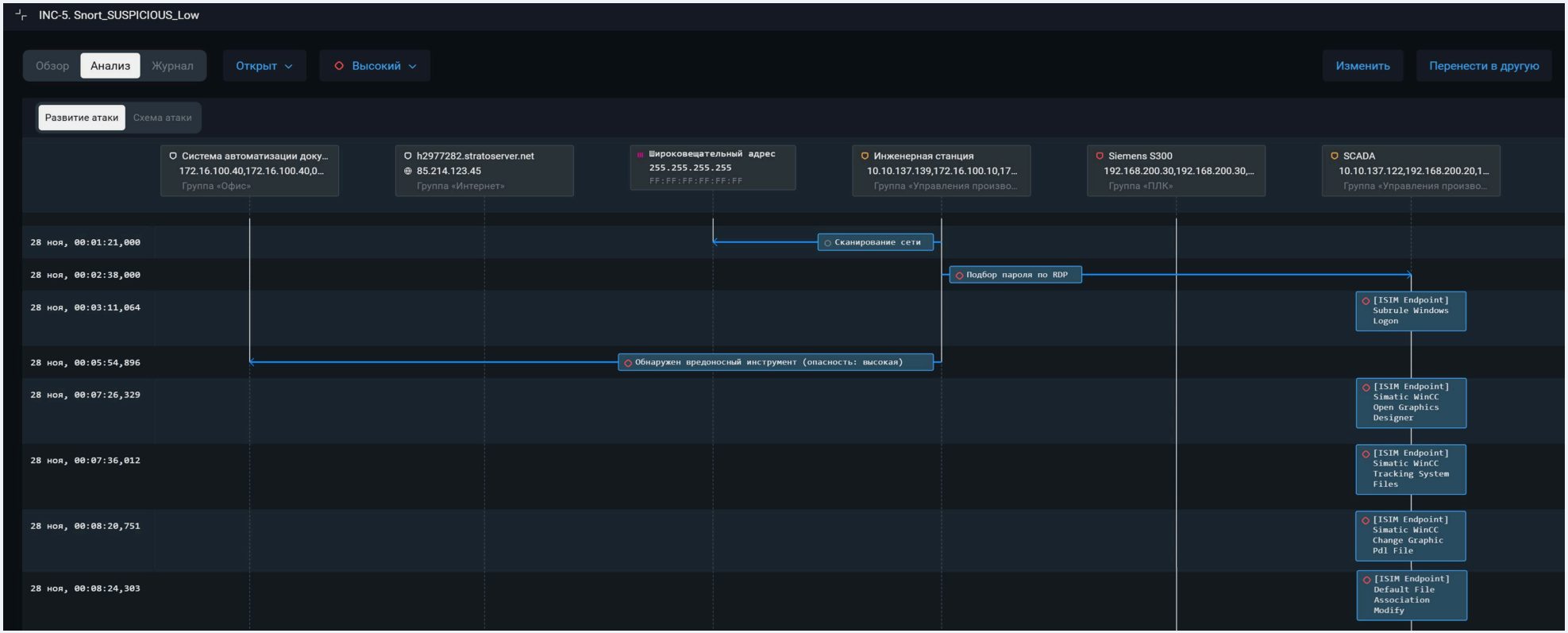
Как отслеживать такие события и реагировать на них

Эффективный способ контроля — использовать SIEM-решение, которое фиксирует модификацию файла проекта вне зависимости от способа внесения изменений. Однако для получения сведений о содержании изменений может понадобиться дополнительное расследование.

Более сложный вариант — отслеживать результат подмены конфигурации, анализируя параметры технологического процесса в сетевом трафике. Например, PT ISIM позволяет создавать настраиваемые пользовательские правила для контроля значений технологических сигналов. Такие правила могут сигнализировать о том, что значение отслеживаемого параметра вышло за допустимый диапазон, или о том, что значение параметра, отвечающего за переключение режима, изменилось.

Дополнительно подозрительные операции с файлами проекта можно выявлять с помощью анализа сетевого трафика. Файлы могут передаваться по сети, а установка проекта из IDE может сопровождаться передачей данных по таким распространенным протоколам, как FTP, TFTP, SMB, HTTP. Обнаружение изменения или передачи файла не обязательно указывает на атаку, но служит основанием для дополнительной проверки и для уточнения информации у специалистов, обслуживающих АСУ ТП.

Рисунок 32. Обнаружение продуктом PT ISIM изменения пароля проекта



На текущем этапе злоумышленники могут закрепиться в системе, чтобы сохранить доступ к ней после перезагрузки или смены пароля. Из-за особенностей Standoff как соревновательного мероприятия участники не использовали эту возможность, однако в реальных атаках это достигается при помощи:

- создания служб;
- внедрения своих конфигураций, ключей или сертификатов в службы удаленного доступа;
- создания задач в планировщике или добавления новых ключей реестра, которые позволяют установить обратное соединение (reverse shell) с C2-сервером;
- добавления пользователей со своими учетными данными.

Как отслеживать такие события и реагировать на них

Необходимо анализировать события в журналах на узлах, отслеживать добавление или изменение ключей реестра и их значений для определенных веток, связанных с функцией автозагрузки. Нужно следить за появлением записей о создании и изменении запланированных задач, о создании локальных учетных записей и изменении локальных групп, а также о создании служб или изменении их состояния.

При обнаружении вредоносной активности необходимо незамедлительно изолировать узел и заблокировать подозрительные соединения на межсетевом экране, остановить подозрительные процессы, удалить нелегитимные учетные записи, сомнительные файлы. Важно также сменить пароли легитимных учетных записей, обеспечить корректность конфигураций сервисов, связанных с получением удаленного доступа, а также проверить целостность и легитимность служб, задач в планировщике, процессов автозапуска.

Этап 4: подготовка инструментов. Этап 5: воздействие на технологический процесс

Если интерфейса SCADA недостаточно, злоумышленники дополнительно устанавливают стороннее ПО для взаимодействия с найденными элементами OT-сети, создают или модифицируют скрипты внутри SCADA-системы для достижения цели.

Финальный этап — выполнение действий, влияющих на технологический процесс. Это может быть остановка оборудования, изменение параметров его работы, повреждение техники, нарушение безопасности производства или вывод системы управления из строя. В рамках кибербитвы Standoff атакующие влияли на технологический процесс двумя разными способами.

Первый способ — воздействие на ПЛК через SCADA-систему. Этот сценарий может быть реализован при помощи запуска модифицированного скрипта или посредством изменения параметров на мнемосхеме[11].

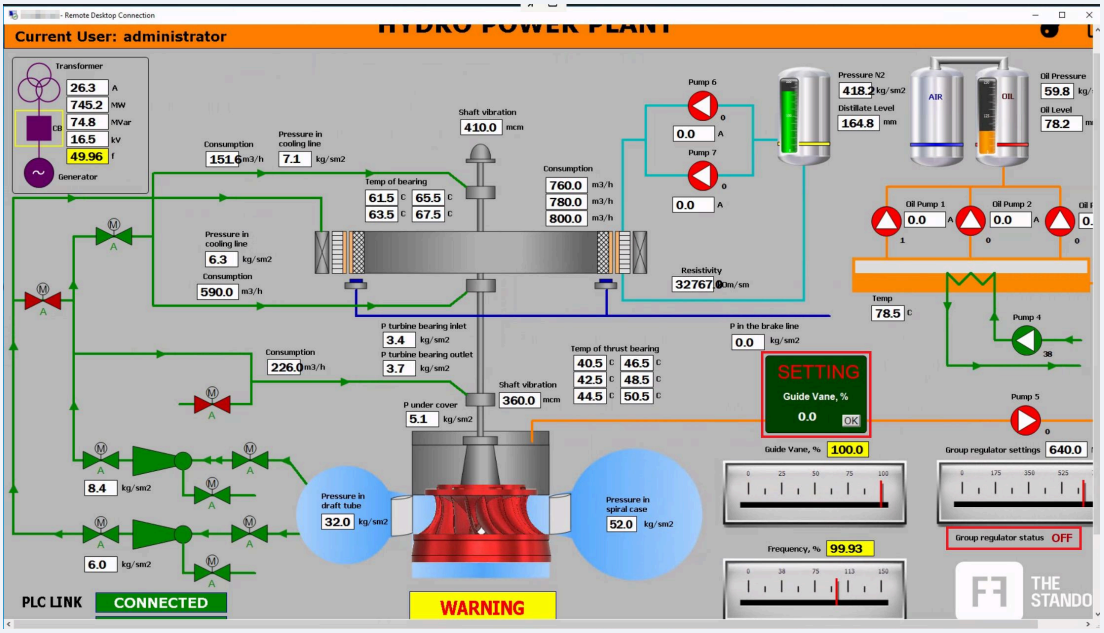
Недопустимое событие «Остановка работы комбината. Нарушение процесса подачи сырья». Атакующие воспользовались редактором Global Script, открыли существующий скрипт *Counter100* и модифицировали его, изменив частоту срабатывания на раз в две секунды и увеличив скорость конвейера. Запуск скрипта привел к нарушению процесса подачи сырья**.**

Недопустимое событие «Остановка работы комбината. Авария на прокатном стане: разрыв заготовки». В папке с проектом *scripts* атакующие создали скрипт *rm.ctl,* в который добавили команду на изменение параметра *PLC_Signal.Set_Cage_T_3* для прокатного стана. Запуск скрипта привел к разрыву заготовки и нарушению режима прокатки.

Недопустимое событие «Прекращение подачи электричества. Остановка работы гидроагрегата на гидроэлектростанции». Атакующие перевели параметр *Group regulator status* на мнемосхеме в выключенное состояние (*ON → OFF*), тем самым отключив автоматическое регулирование работы гидроагрегата. А действием *Guide Vane: 80.0 → 0.0* они закрыли направляющие лопатки и остановили турбину.

[11] Мнемосхема — условное графическое отображение технологических процессов, поточно-транспортных линий, энергетических и других систем.

Рисунок 33. Мнемосхема с измененными красной командой параметрами



Угроза: подмена файла проекта в системах SCADA и HMI

Как отслеживать такие события и реагировать на них

В приведенных примерах результат подмены конфигурации также необходимо контролировать через анализ параметров технологического процесса в сетевом трафике.

Второй способ — воздействие на ПЛК посредством отправки команд к нему напрямую или с использованием специализированного ПО.

Недопустимое событие «Остановка конвейера и разлив краски на лакокрасочном заводе». Красная команда установила программное обеспечение для управления ПЛК. Такие утилиты есть у большинства вендоров АСУ ТП и легитимно используются инженерами для диагностики, обнаружения и настройки устройств. Атакующие могут использовать эти инструменты для разведки и воздействия на производственный процесс.

Далее атакующие подключились к ПЛК и с помощью развернутого ПО изменили тег[12], отвечающий за остановку линии. Это привело к разливу краски и выводу оборудования из строя.

Угроза: запуск инженерного и управляющего ПО в АСУ ТП

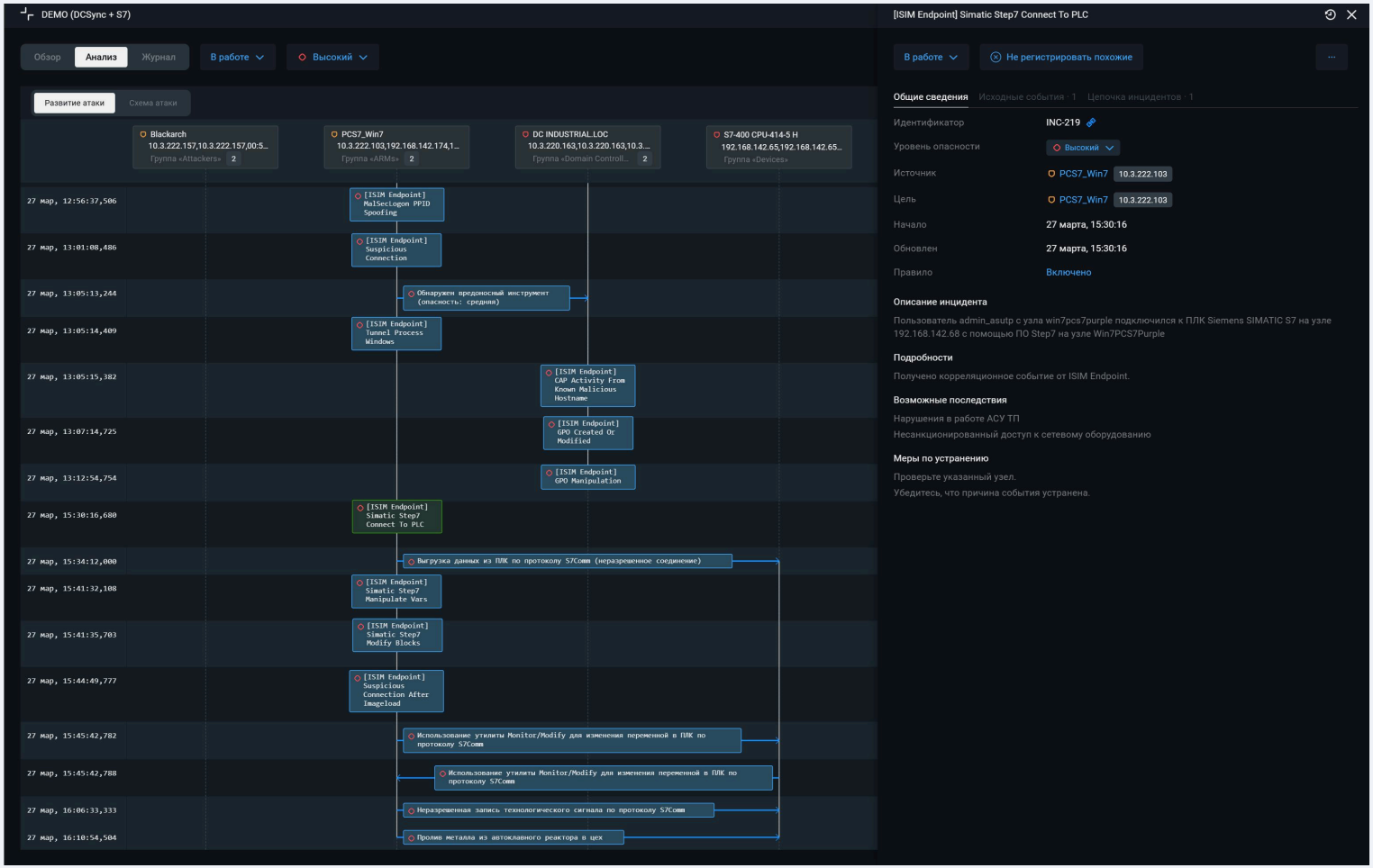
Как отслеживать такие события и реагировать на них

Запуск инженерного и управляющего ПО можно отслеживать с помощью SIEM-, EDR- или EPP-решений по событиям запуска процессов. Часто запуск сопровождается появлением в трафике управляющих протоколов, поэтому отслеживание соединений позволяет обнаружить нелегитимное использование утилит там, где нет сбора событий SIEM-системой и не стоит средство защиты конечных точек.

Факт запуска инженерного и управляющего ПО не всегда свидетельствует о присутствии злоумышленника: операции может выполнять обслуживающий персонал. Однако обычно настройка происходит в строго оговоренные промежутки времени — технологические окна — и вне этих периодов не проводится. Поэтому появление такой активности требует проверки.

[12] Тегами, или технологическими сигналами, обычно называют переменные в памяти ПЛК, в которых содержится либо текущее значение измеряемого физического показателя, либо режим работы того или иного подпроцесса в ПЛК. Иными словами, записывая или читая теги, SCADA-система и ПЛК обмениваются командами и индикациями

Рисунок 34. Пример обнаружения продуктом PT ISIM запуска инженерного ПО



Угроза: неавторизованное чтение и запись тегов в ПЛК

Как отслеживать такие события и реагировать на них

Обнаружить неавторизованное взаимодействие по технологическому протоколу (например, когда к ПЛК обращается ранее неизвестный узел) относительно просто при использовании средств анализа технологического трафика, которые позволяют определить тип протокола и выполняемые команды. Реагирование заключается в проверке легитимности подключения совместно со специалистами, обслуживающими АСУ ТП.

Сложнее выявить подозрительные действия с авторизованных узлов, так как внешне активность не отличается от штатной работы. В таких случаях целесообразно применять правила или механизмы для автоматического профилирования и выявления аномалий.

Рисунок 35. Пример обнаружения продуктом PT ISIM неавторизованного взаимодействия по технологическому протоколу

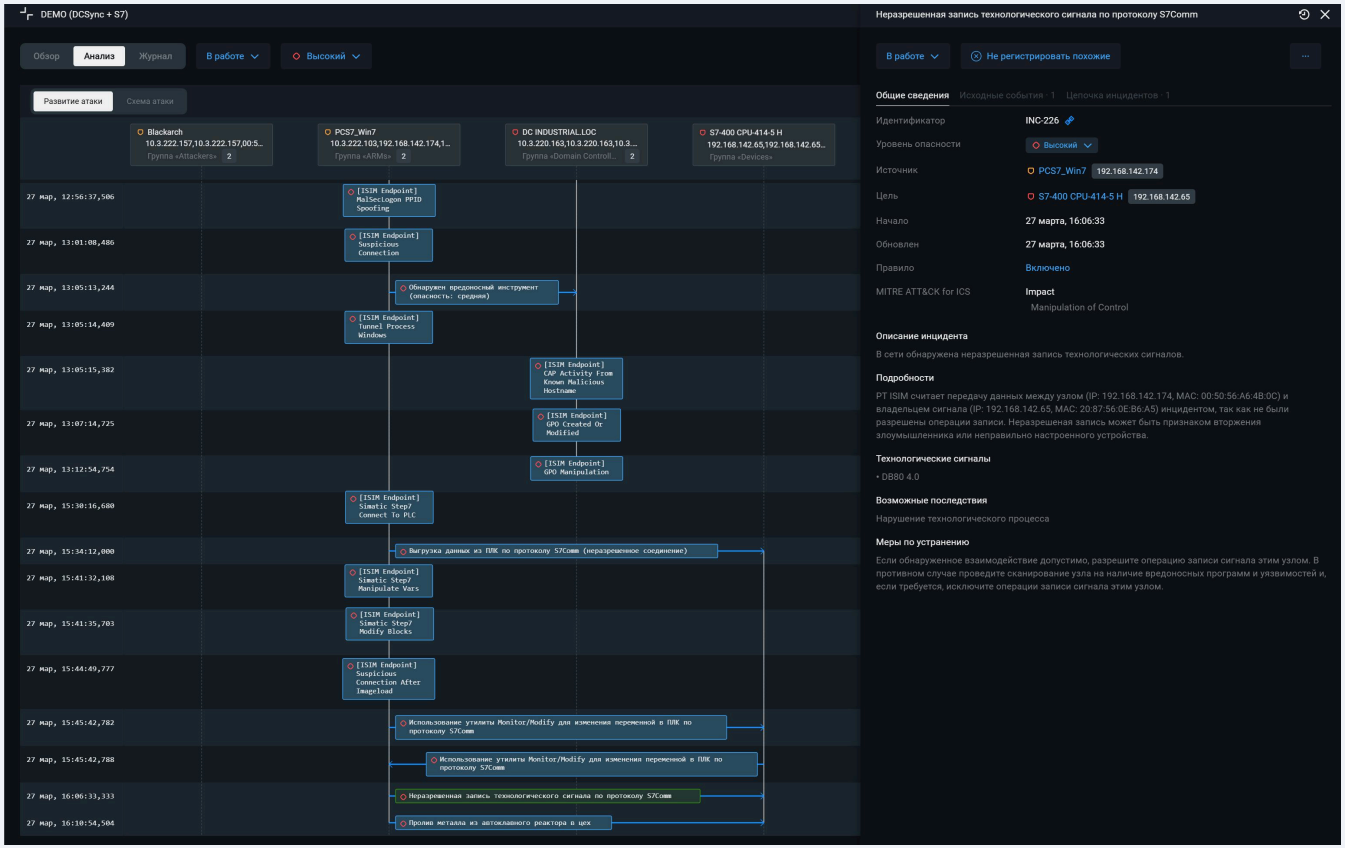
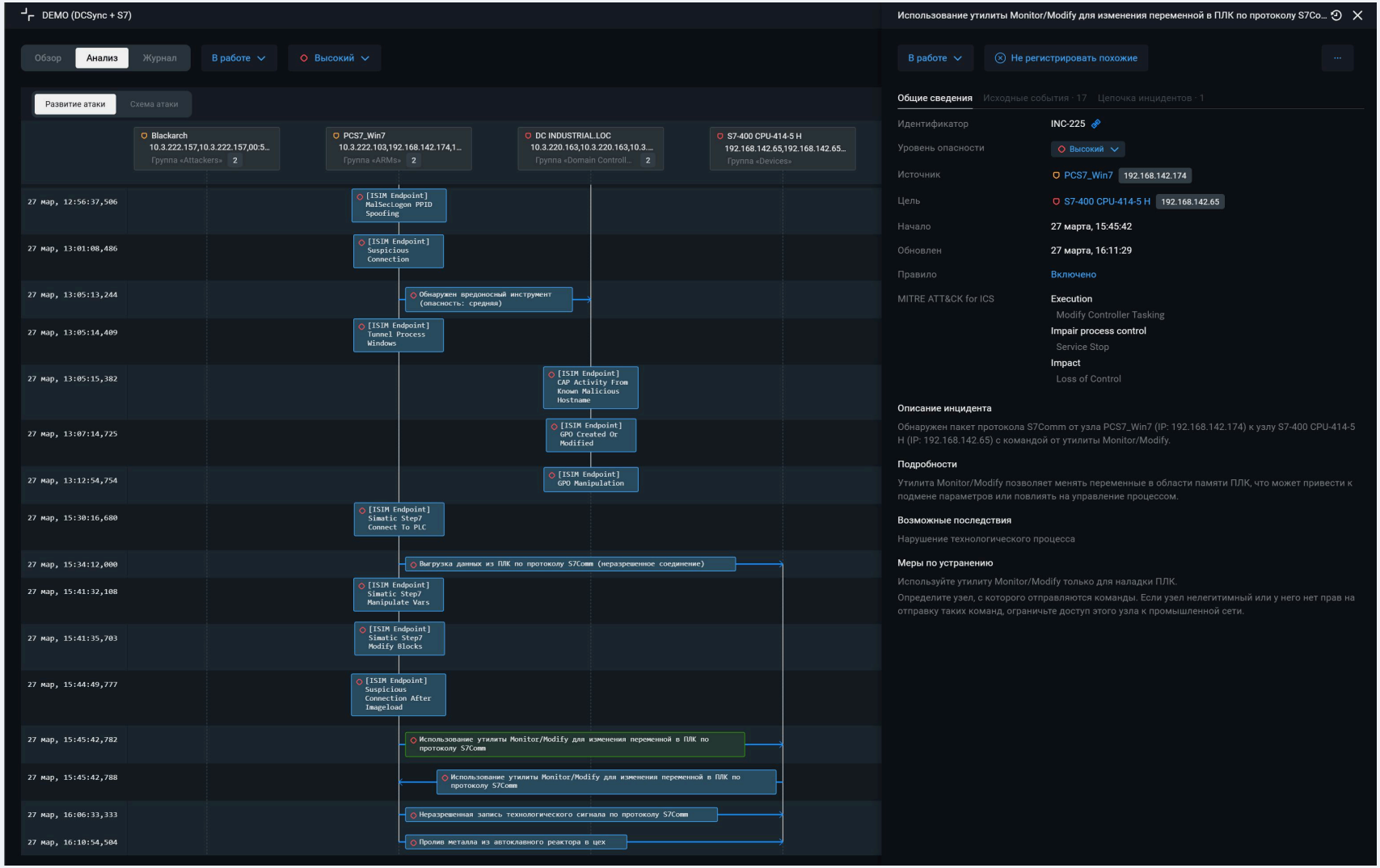


Рисунок 36. Пример обнаружения продуктом PT ISIM изменения параметра переменной в ПЛК



Недопустимое событие «Остановка нефтеперекачивающей станции». Атакующие установили программу Modbus Poll[13] для управления контроллером, после чего отправили на него команду — в результате произошла остановка станции.

Стоит отметить, что протокол Modbus, широко используемый на промышленных предприятиях, является слабо защищенным. Изначально он был разработан без встроенных механизмов аутентификации, шифрования данных и проверки целостности. Поэтому фактически любой пользователь устройства, имеющего сетевой доступ к ПЛК, может послать ему тот же сигнал, что и SCADA-система. По данным Forescout, Modbus стал причиной 57% атак с использованием протоколов OT в 2025 году.

Угроза: использование слабозащищенных версий протоколов

Как отслеживать такие события и реагировать на них

Отслеживать использование слабых протоколов можно с помощью активного аудита и анализа трафика. Реагирование на обнаружение уязвимых протоколов зависит от условий: их можно заменить на защищенные версии, однако в случае, когда бесшовно провести такое обновление нельзя, их можно сохранить, но учесть наличие слабых мест при мониторинге.

[13] Modbus Poll — популярная программа-симулятор ведущего устройства (master) для протокола Modbus, предназначенная для тестирования, отладки и мониторинга ведомых устройств (slave), таких как ПЛК, датчики или модули ввода-вывода.

Рисунок 37. Пример обнаружения продуктом PT ISIM использования устаревшего протокола SNMP

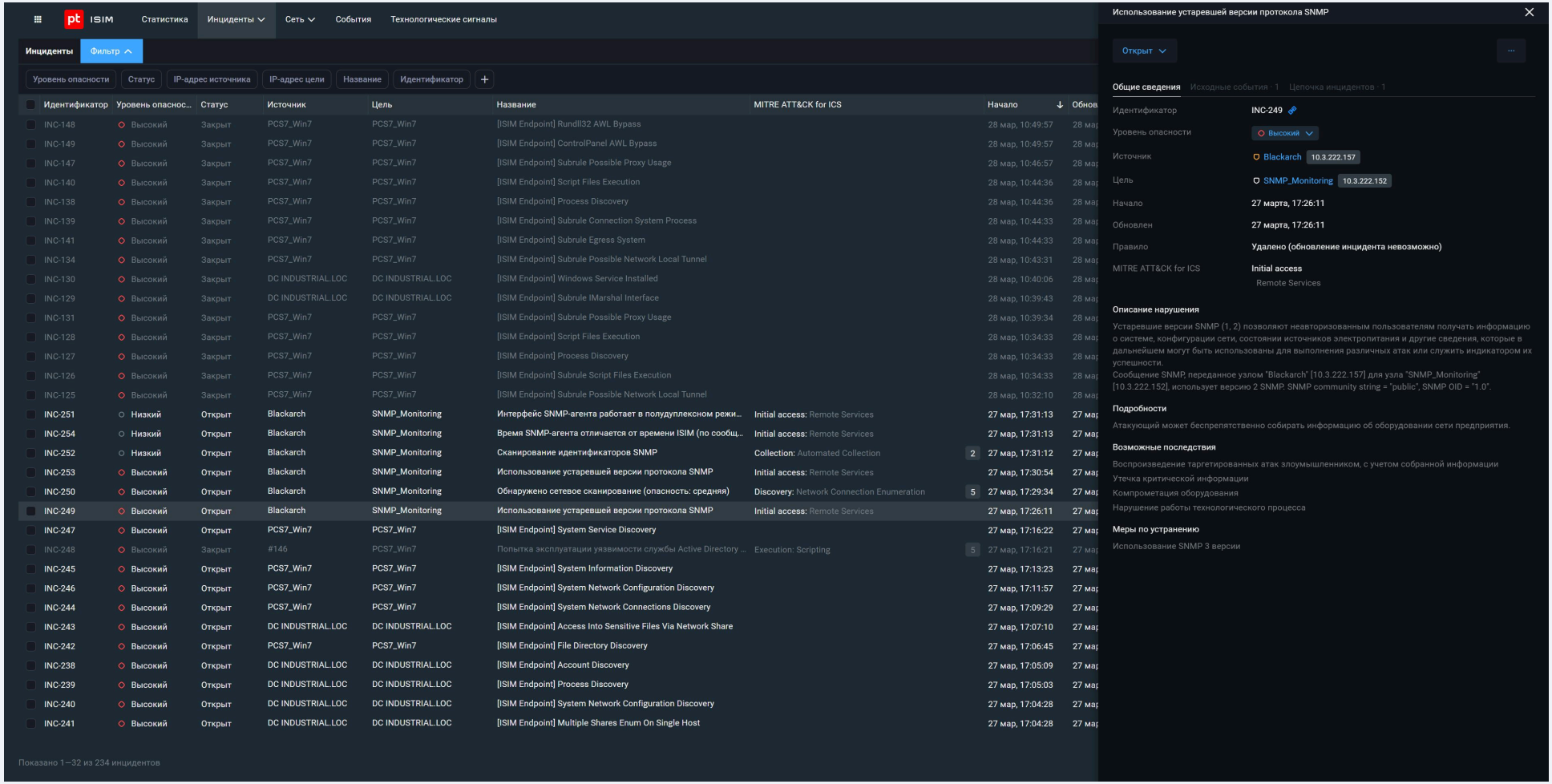
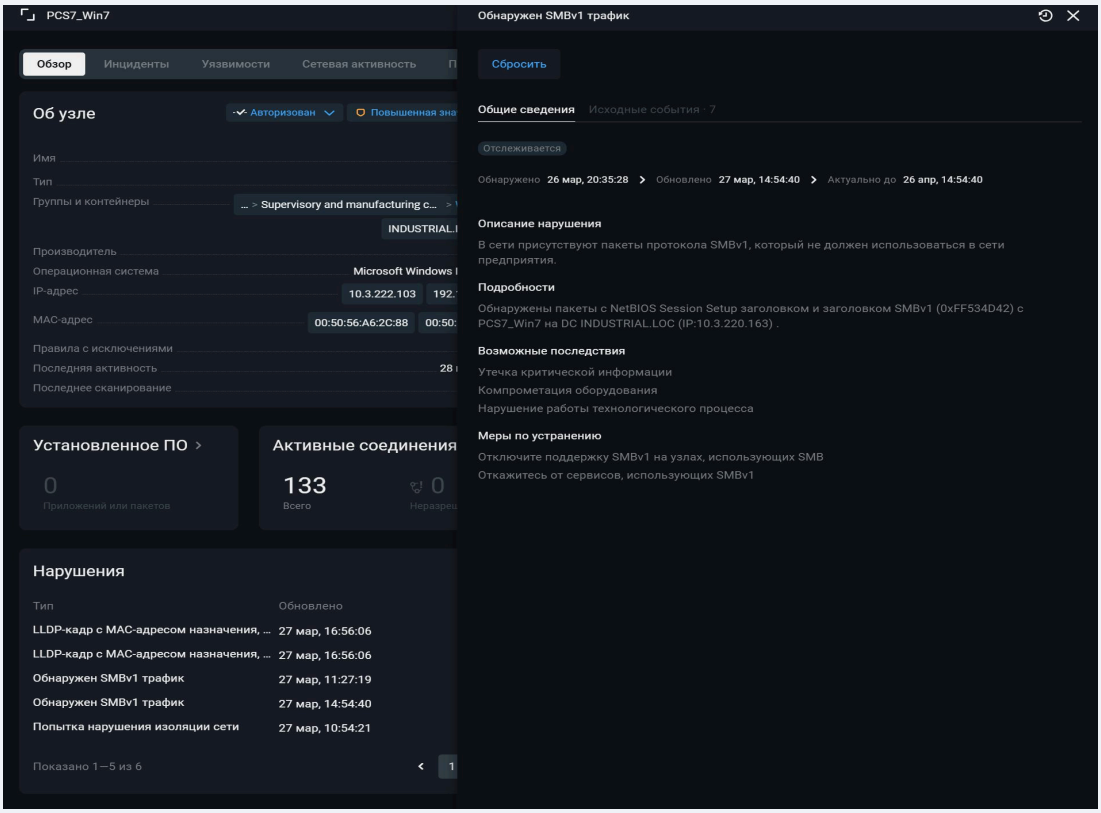


Рисунок 38. Пример обнаружения продуктом PT ISIM использования устаревшего протокола SMBv1



Другие этапы атаки на технологический сегмент

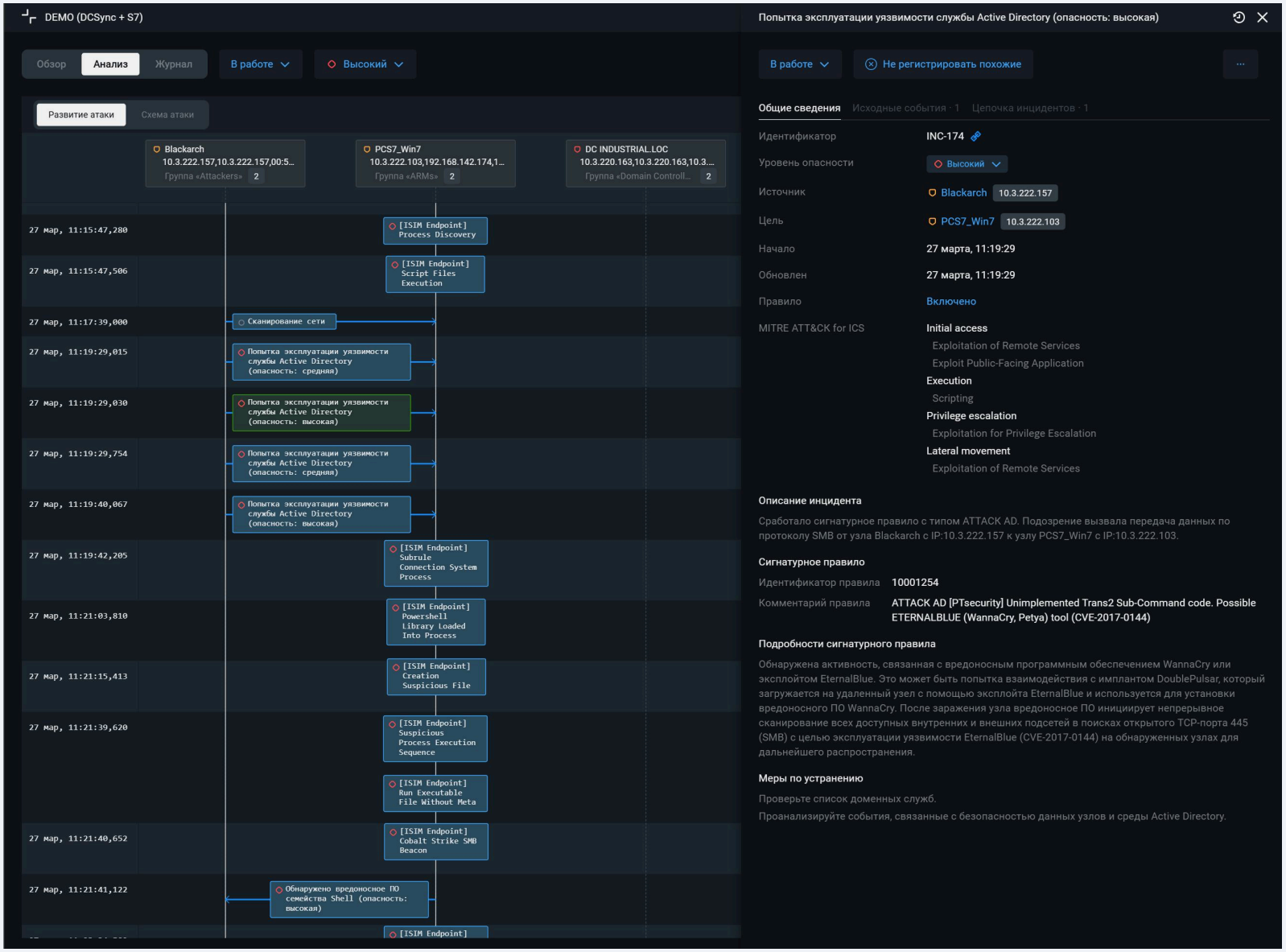
В реальных случаях прямое воздействие на технологический процесс происходит далеко не всегда. Устройства верхнего уровня технологической сети — это обычные компьютеры с Windows и Linux (нередко устаревших версий). Атакуя их, злоумышленники могут нарушить и технологический процесс.

Угроза: активность ВПО, атаки на ОС, ПО, сетевое оборудование

Как отслеживать такие события и реагировать на них

Система обеспечения информационной безопасности в технологическом сегменте должна включать экспертные правила, позволяющие выявлять характерные для Windows и Linux угрозы: активность ВПО, эксплуатацию уязвимостей, сетевые и локальные атаки, запуск подозрительных утилит. Правила обычно точно указывают на наличие угрозы, однако в отдельных случаях могут срабатывать на легитимную активность, поэтому требуют дополнительной настройки.

Рисунок 39. Пример обнаружения продуктом PT ISIM эксплуатации уязвимости EternalBlue (CVE-2017-0144)



Важно сказать, что атаки на ИТ-сегмент могут повлиять на остановку технологического процесса. Например, так произошло с немецким производителем аккумуляторов VARTA AG: из-за кибератаки пришлось отключить часть ИТ-систем, что в итоге привело к остановке производства на пяти заводах. Спустя две недели доступность систем все еще была ограничена.

Как мы отметили ранее, в рамках соревнований Standoff невозможно реализовать все этапы атаки на ОТ. Однако в реальных инцидентах также достаточно часто встречаются:

- **Сбор и анализ данных о процессе.** Наблюдение за работой предприятия для понимания нормального поведения процесса перед вредоносным воздействием.
- **Манипуляция показаниями.** Подмена отображаемых на мнемосхеме значений для того, чтобы запутать оператора, когда технологический процесс уже нарушен. Это может привести к проблемам, которых оператор даже не заметит. Или же может произойти наоборот: оператор предпримет меры для стабилизации несуществующей ситуации — и они в итоге негативно повлияют на технологический процесс.
- **Вывод защитных систем из строя.** Отключение или блокировка систем противоаварийной защиты перед воздействием.
- **Уничтожение следов после атаки.** Очистка журналов SCADA-системы, журнала событий Windows, удаление установленного ПО. Киберпреступники делают это, чтобы скрыть следы своего присутствия, затруднить расследование инцидента и избежать обнаружения.
- **Перемещение внутри ОТ-сети.** Переход с одного ПЛК или SCADA-узла на другой внутри ОТ-сети при помощи RDP и SSH. Это действие можно отследить по протоколам удаленного доступа, как и в случае с получением злоумышленниками доступа из ИТ-сегмента к ОТ-сегменту.

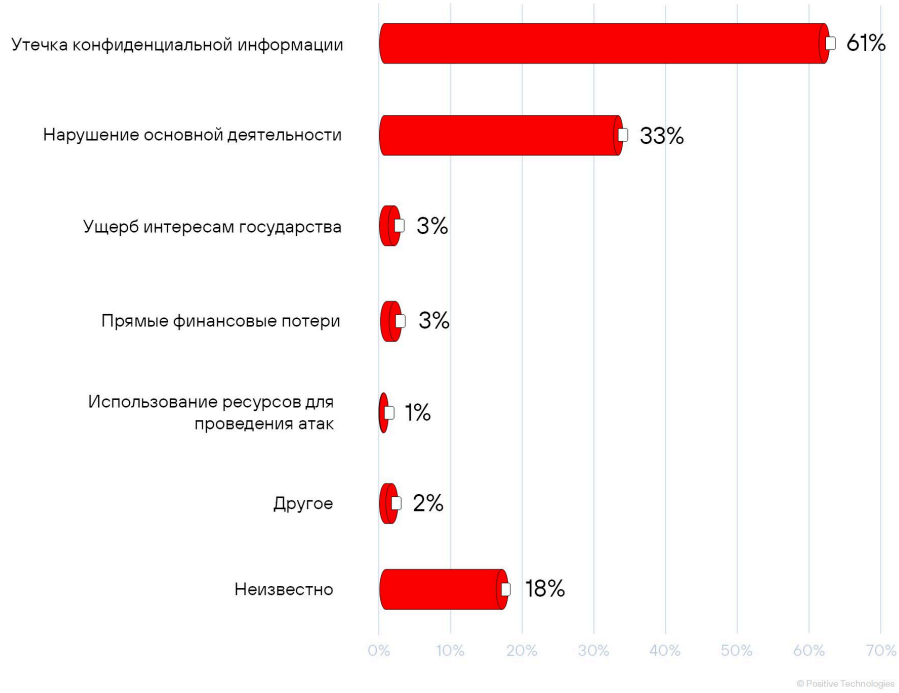
Таким образом, атака на технологический сегмент представляет собой последовательный сценарий от получения первоначального доступа до воздействия на производственный процесс. Детальное рассмотрение таких сценариев показывает, что атака на технологический сегмент — это не черный ящик и не совокупность уникальных, не поддающихся обнаружению действий. Напротив, даже самые сложные сценарии развиваются через наблюдаемые этапы, которые можно выявить при наличии нужной экспертизы и специализированных средств анализа событий и трафика, а также при корректно выстроенной архитектуре мониторинга.

Защита OT-сегмента не должна строиться вокруг одного класса средств. Необходим комплексный подход, обеспечивающий видимость инфраструктуры, контроль изменений и возможность выявлять опасные действия до наступления недопустимого события.

Последствия атак

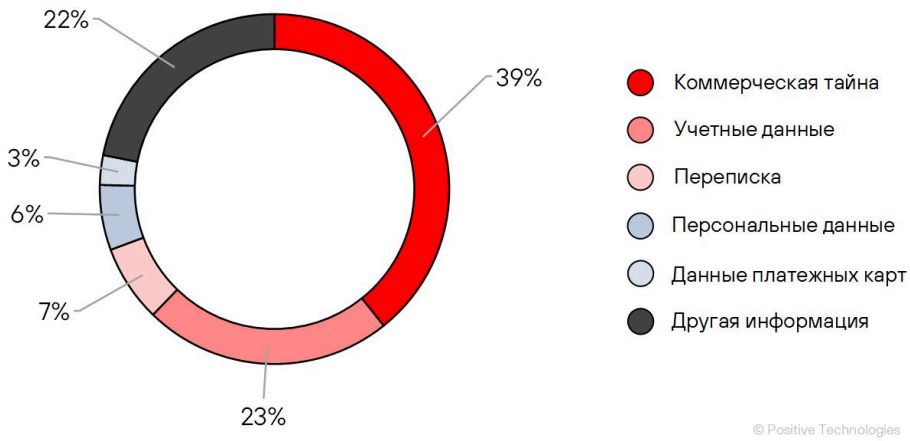
Успешные атаки на отечественный промышленный сектор чаще всего, а именно в 61% инцидентов, приводили к утечкам конфиденциальной информации.

Рисунок 40. Последствия атак на российские промышленные организации (доля успешных атак, 2024–2025)



В совокупности в российских организациях наиболее часто фиксировались утечки коммерческой тайны (29%). В промышленном секторе наблюдается аналогичная картина, однако доля случаев кражи этой информации существенно превосходит общероссийский показатель (на 10 п. п.). Повышение интереса к коммерческой тайне пришлось на снижение числа инцидентов, связанных с утечкой персональных данных: в то время как в отношении российских организаций доля хищения персональной информации составляла 16%, в секторе производства она была украдена в 6% случаев. Причина в том, что в промышленном секторе акценты смещены: злоумышленников интересует техническая документация, сведения о разработках и ноу-хау. В отличие от персональных данных, которые часто можно найти во множестве разных баз, технологическая информация уникальна и зачастую невосполнима. Кроме того, промышленные предприятия реже хранят массивы персональных данных.

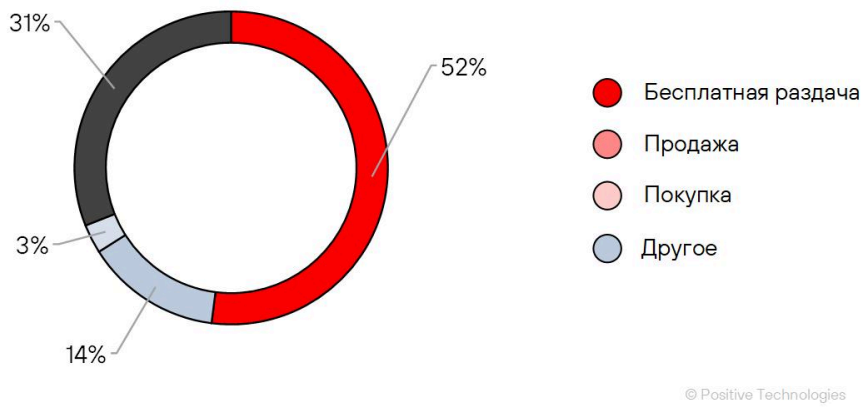
Рисунок 41. Типы украденных данных в успешных атаках на российские промышленные организации (2024–2025)



Почти четверть (23%) инцидентов на промышленных предприятиях закончилась утечками учетных данных — они могут быть использованы для дальнейшего развития атаки. В связи с высоким числом краж этих сведений можно предположить, что в 2026–2027 годах кибератак, в которых они будут применяться, станет больше.

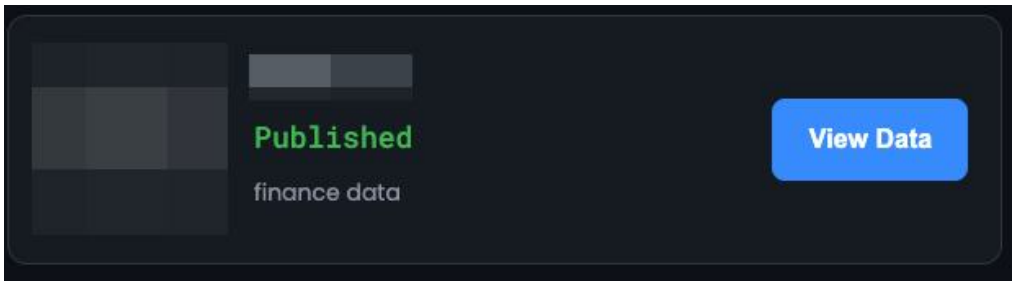
Похищенные сведения не всегда остаются исключительно в руках злоумышленников. Так, более половины объявлений (52%), связанных с утечками из российских промышленных организаций, представляют собой бесплатную раздачу украденных данных. Часть объявлений опубликована хактивистами, которые сливают информацию в даркнет без преследования финансовой выгоды; другая часть — финансово мотивированными злоумышленниками, которые могут использовать данные несколькими способами. К примеру, атакующие публикуют похищенные материалы, если организация отказывается от выплаты выкупа, — для усиления негативных последствий. Данные также могут служить инструментом давления: киберпреступники выкладывают часть базы в даркнет и обещают опубликовать оставшуюся в случае неуплаты. Стоит отметить, что значительная доля (73%) объявлений имела отношение к раздаче небольшого объема информации — до 1 ГБ.

Рисунок 42. Типы объявлений, связанных с утечками данных из российских промышленных организаций, на теневых форумах (2024–2025)



Встречались объявления о бесплатной раздаче более крупных архивов со сведениями (27%) — размером от 1 ГБ до 1 ТБ. Так, злоумышленники опубликовали данные компании, предоставляющей решения для АЭС, среди которых были адреса почты сотрудников, внутренние документы, финансовые отчеты, выгрузки из системы «1С». Вероятно, ситуация произошла после отказа жертвы выплатить выкуп.

Рисунок 43. Опубликованные данные компании, предоставляющей решения для АЭС



Раздавались преимущественно персональные данные (82%): такая информация может иметь низкую коммерческую ценность и дублироваться в других утечках. В то же время более чувствительные материалы — техническая документация, производственные схемы, сведения о разработках и иная внутренняя информация — сохраняются для последующей продажи или другого использования. Опубликованные персональные данные могут выступать инструментом давления или способом привлечь внимание, создавать для компании серьезные репутационные издержки и риски крупных штрафов в условиях ужесточения законодательства.

Седьмая часть объявлений (14%) связана с продажей украденной из промышленных организаций информации. В двух третьих (67%) случаев размер утечек был значительным — от 100 тыс. до 1 млн записей. В части объявлений к покупке предлагались учетные данные (50%), внутренние файлы (33%) и исходный код (33%). Например, эти сведения содержались в самой дорогой утечке — стоимостью 300 тыс. долларов (о ее составе мы рассказали ранее).

Во всех объявлениях, связанных с продажей информации, содержались архивы с персональными данными. Например, к покупке предлагался список акционеров одной из российских нефтяных компаний. Продавец утверждал, что база содержит персональные данные почти 60 тыс. человек, а также сведения о начисленных дивидендах. В качестве подтверждения подлинности данных был размещен семпл базы.

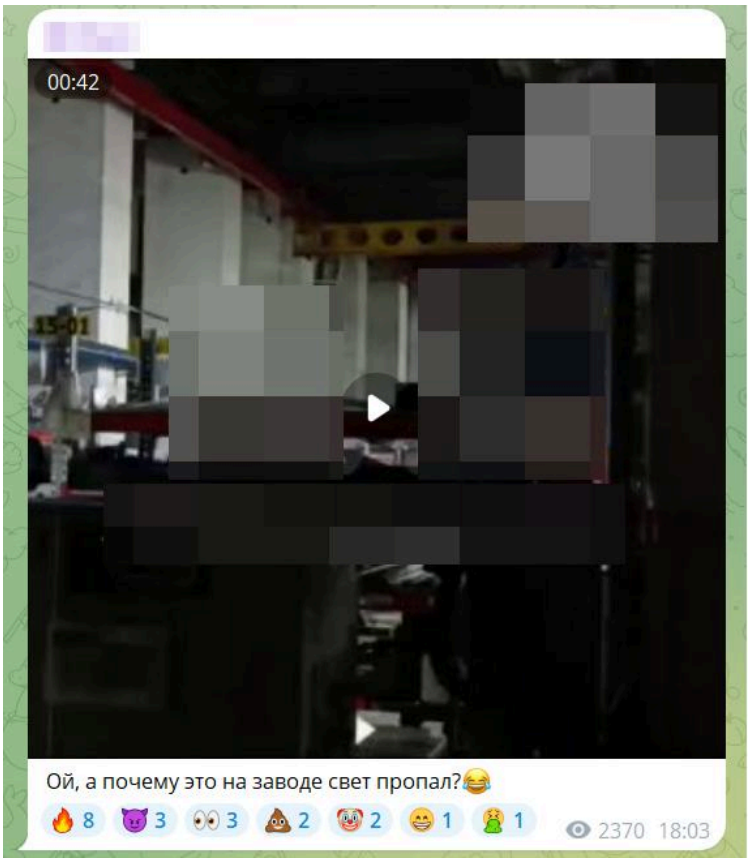
Рисунок 44. Объявление о продаже списка акционеров российской нефтяной компании

Интересно, что в части объявлений, связанных с приобретением информации, покупателей интересовали именно акционеры. Данные о них могут представлять ценность для злоумышленников, поскольку это не просто набор имен, а база людей, связанных с капиталом, инвестициями и, возможно, корпоративными структурами. Получив подобные сведения, киберпреступники могут проводить точечный фишинг, инвестиционные аферы, а также разведку для дальнейшей атаки на компанию.

Помимо утечек данных, главным серьезным последствием кибератак для российских промышленных компаний стало нарушение основной деятельности (33%). Так, в результате кибератаки злоумышленники вызвали сбои в работе российского агрокомплекса и потребовали выкуп в размере 500 млн рублей. Другой пример — инцидент в одной из компаний ТЭК: сотрудникам было предписано не заходить в рабочие аккаунты во избежание утечки, а у клиентов АЗС возникли проблемы при попытке оплаты картами. По данным СМИ, атака была вызвана вирусом-шифровальщиком.

Еще один пример — кибератака хактивистской группировки на одного из производителей сельскохозяйственной техники: преступники сообщили о выведении из строя серверов и компьютеров сотрудников, об уничтожении и шифровании более 200 ТБ данных, в том числе резервных копий. Позже в одном из Telegram-каналов было опубликовано сообщение о том, что на предприятии перестало работать электричество.

Рисунок 45. Пост хактивистов с сообщением об отключении электричества на атакованном предприятии



Нарушение деятельности промышленных предприятий нередко вызывает цепочку каскадных последствий: приводит к сбоям в логистике, к нарушению графика поставок и отгрузок. Срыв сроков может повлечь за собой невыполнение контрактных обязательств и, как следствие, штрафные санкции. В результате киберинцидент становится причиной не только технических неполадок, но и юридических и финансовых проблем.

Показательный случай произошел в мае 2025 года с немецким производителем Fasana. Кибератака парализовала системы компании, остановила производство и обработку заказов на сумму свыше 250 тыс. евро, заставила задержать выплату зарплат. Две недели простоя привели к потере около 2 млн евро — организация объявила о банкротстве.

Как защититься

Защита промышленных предприятий невозможна без одновременного обеспечения безопасности корпоративного и технологического сегмента с учетом их взаимодействия.

Защита корпоративного сегмента

Почти три четверти атак (71%) на отечественные промышленные предприятия происходили с применением методов социальной инженерии. Поэтому обучение персонала практикам кибербезопасности является ключевым шагом в выстраивании эффективной защиты.

В 83% успешных кибератак на производственные организации в России злоумышленники применяли вредоносное программное обеспечение, для рассылки которого использовали электронную почту, сайты, мессенджеры и социальные сети. Чтобы минимизировать шансы на успешную доставку ВПО, мы рекомендуем:

- использовать почтовые и веб-шлюзы, проверяющие вложения и ссылки в электронных письмах в режиме реального времени;
- внедрить NGFW и прокси-сервисы с функцией категоризации сайтов и фильтрацией трафика — например, PT NGFW;
- контролировать каналы обмена файлами внутри организации, включая мессенджеры, где возможна доставка ВПО с использованием социальной инженерии;
- регулярно тестировать параметры шлюзов и фильтров с помощью специализированных решений, имитирующих реальные сценарии доставки ВПО.

Примерно в трети (28%) успешных кибератак на российские промышленные организации киберпреступники эксплуатировали уязвимости — как довольно старые, так и трендовые. Своевременное устранение недостатков — важная задача в обеспечении защиты системы. Продукты класса VM позволяют обнаруживать слабые места до того, как ими воспользуется злоумышленник, помогают правильно расставить приоритеты их устранения, а также автоматизировать процесс обновления.

В 9% киберинцидентов в отечественных компаниях производственного сектора злоумышленники использовали методы, связанные с компрометацией учетных данных. Для минимизации риска необходимо использовать стойкие пароли: установите требования к их сложности, исключающие возможность применения словарных комбинаций. Не нужно хранить пароли в открытом виде — можно использовать специальный менеджер. Рекомендуется включить двухфакторную аутентификацию для всех публично доступных сервисов (для подключения к VPN, входа в электронную почту и т. п.), а также сделать ее обязательной для всех административных учетных записей в корпоративной сети.

Эффективная защита ИТ-инфраструктуры невозможна без знания обо всех активах и данных в ней. Забытые сервисы, неучтенные устройства, теневые системы и устаревшие компоненты — все это становится точками входа в инфраструктуру. Поэтому необходимо своевременно выявлять такие уязвимые элементы, обновлять их или исключать из эксплуатации, если они больше не нужны. Для этого рекомендуем использовать технологии asset management.

Чтобы обеспечить соблюдение политик безопасности на уровне узлов, сетевых ресурсов и учетных записей, рекомендуется применять решения класса host compliance control (HCC), network compliance control (NCC) и user compliance control (UCC):

- HCC-системы позволяют контролировать, что на активах соблюдаются парольная политика, требования к ведению журналов значимых системных событий, к защите от сетевых атак.
- NCC-решения нужны для обеспечения безопасности сетевых ресурсов: они помогают привести конфигурацию сетевых устройств в соответствие политикам безопасности, сегментировать сеть, придерживаться использования защищенных протоколов.
- Средства класса UCC предназначены для защиты учетных записей пользователей, для предотвращения компрометации учетных данных и для контроля доступа к информационным системам.

Чтобы прогнозировать сценарии продвижения злоумышленников в инфраструктуре и своевременно реагировать на угрозы, рекомендуется использовать комплексные системы, объединяющие функциональность всех перечисленных решений.

Для мониторинга и своевременного реагирования на угрозы следует использовать SIEM-системы, обеспечивающие сбор и анализ событий безопасности из различных источников. Рекомендуется применять решения класса EDR и EPP для обнаружения событий, связанных с вредоносной активностью на конечных устройствах, а также NTA-системы, предназначенные для анализа сетевого трафика. Обнаруживать угрозы в почтовом трафике, реагировать на них можно с помощью PT Email Security — решения для статистического и динамического анализа угроз и выявления сложного вредоносного ПО.

Если самостоятельно организовать SOC (security operations center) для круглосуточного мониторинга и реагирования невозможно, рекомендуем воспользоваться услугами сторонних профильных компаний. Кроме того, можно рассмотреть решения для круглосуточного мониторинга и реагирования на киберугрозы.

Для получения знаний об актуальных угрозах ИБ рекомендуем подписаться на фиды threat intelligence, а также использовать порталы с данными о киберугрозах. Благодаря ним можно обогатить средства защиты данными и повысить их эффективность, что позволит обнаруживать и предотвращать атаки на ранних этапах.

Неотъемлемая часть работы, связанной с поддержанием киберустойчивости, — регулярная оценка защищенности ИТ-инфраструктуры, по результатам которой формируется план устранения выявленных недостатков. В зависимости от целей, уровня зрелости процессов информационной безопасности и этапа жизненного цикла объекта доступны разные способы оценки: предприятие может воспользоваться специализированными услугами, выполнить ретроспективный анализ событий ИБ, провести тестирование на проникновение (пентест), в том числе автоматизированное, или организовать киберучения.

Более половины (61%) атак на компании в 2025 году закончились утечкой конфиденциальной информации, поэтому важной задачей в укреплении ИТ-инфраструктуры становится защита данных. Рекомендуем использовать продукты, обеспечивающие полную видимость инфраструктуры их хранения и обработки.

В случае если инцидент все же произошел, рекомендуем провести ретроспективный анализ с целью установления причин атаки, вектора проникновения и масштабов компрометации. Это позволит выявить слабые места в инфраструктуре и выработать меры защиты, которые помогут предотвратить аналогичные ситуации в будущем.

Защита технологического сегмента

Защита технологического сегмента должна выстраиваться с учетом специфики технологических процессов и их значимости для непрерывной работы предприятия. Процессы ИБ в промышленной среде должны быть частью системы, а не внешней надстройкой: требования к безопасности необходимо закладывать уже на этапе построения или модернизации технологического сегмента. На практике это означает, что его защита требует сочетания классической экспертизы в области информационной безопасности и глубокого понимания особенностей технологической среды: архитектуры АСУ ТП, логики процессов, типов недопустимых событий и ограничений эксплуатации. Только так возможно построить действительно работающую модель киберустойчивости для промышленного предприятия.

В подобных условиях для защиты промышленной инфраструктуры недостаточно разрозненных средств, каждое из которых решает лишь отдельную задачу. Необходим комплексный подход, который учитывает специфику технологической среды и позволяет видеть инфраструктуру, риски и развитие атаки в едином контексте. Именно такой подход реализован в PT ISIM. Система объединяет функции, необходимые для комплексной защиты технологического сегмента, включая инвентаризацию активов и контроль изменений, управление уязвимостями, защиту конечных узлов, антивирусную защиту, мониторинг технологической сети и контроль параметров технологического процесса, — то, что при традиционном подходе выполняют решения разных классов: asset management, vulnerability management, EDR и других.

- **Инвентаризация технологической сети и выявление уязвимостей.** PT ISIM формирует актуальную картину технологической инфраструктуры и помогает оценивать текущее состояние защищенности. Система собирает и контролирует инвентаризационные данные о программном и аппаратном обеспечении, позволяет собирать информацию о пользователях и группах, обнаруживает новые узлы — рабочие станции, контроллеры и сетевые устройства, анализирует защищенность компонентов АСУ ТП и отслеживает изменение конфигураций оборудования и ПО.

- **Контроль целостности технологической сети.** PT ISIM обеспечивает постоянный контроль сетевой инфраструктуры АСУ ТП: выявляет неизвестные устройства, несанкционированные подключения, фиксирует соединения с внешними IP-адресами за пределами технологической сети, контролирует корректность списков доступа на межсетевых экранах, выявляет нарушения периметра и анализирует взаимодействия по общесетевым и промышленным протоколам. В удаленных и изолированных сегментах, включая сегменты за диодом данных, для сбора и обработки сетевого трафика в рамках централизованного мониторинга безопасности может применяться PT ISIM Collector.

- **Обнаружение аномалий и угроз в трафике технологической сети.** Продукт в режиме реального времени выявляет отклонения в сетевой активности и признаки компрометации. Система обнаруживает вредоносную активность и распространение вирусов, использование прокси-серверов и сетевых туннелей, слабые и установленные по умолчанию пароли, небезопасные и устаревшие протоколы, а также атаки на сетевые устройства и системы на базе Windows и Linux.

- **Защита конечных узлов.** PT ISIM обеспечивает антивирусную защиту рабочих станций и серверов АСУ ТП, анализирует события безопасности на серверах и АРМ для выявления внешних и внутренних угроз. Помогает выявлять несанкционированный доступ к данным и обнаруживать атаки типа living off the land, при которых злоумышленник использует легитимные инструменты.

- **Защита SCADA-систем.** За счет промышленной экспертизы PT ISIM позволяет выявлять атаки на распространенные российские и зарубежные SCADA-системы, включая подмену исполняемых файлов и файлов проектов, подбор паролей, нелегитимный запуск инженерного ПО, изменение конфигураций и критически важных сервисов.

- **Контроль параметров технологического процесса.** Продукт контролирует действия, влияющие на безопасность и стабильность технологического процесса, и помогает выявлять попытки скрытого вмешательства. PT ISIM фиксирует отклонения ключевых технологических показателей от безопасных значений, позволяет задавать правила для контроля критически значимых параметров, выявляет отправку важных управляющих команд и обнаруживает опасные технологические команды, в том числе команды на перепрошивку ПЛК, на форсирование переменных и очистку памяти.

- **Соответствие требованиям регулирующих организаций.** PT ISIM позволяет соблюсти требования ФСТЭК к антивирусной защите объектов критической информационной инфраструктуры (КИИ), а также выстроить взаимодействие с центрами ГосСОПКА.

В совокупности эти возможности дают предприятию полную видимость технологической среды, позволяют выявлять угрозы, аномалии, уязвимости и конфигурационные риски, контролировать параметры технологического процесса и повышать устойчивость промышленной инфраструктуры к кибератакам.

Для более детальной проработки подхода к построению надежной защиты можно обратиться к методическому руководству OT Cybersecurity Framework, разработанному экспертами Positive Technologies и посвященному построению комплексных систем кибербезопасности промышленной инфраструктуры.

Возросшее число кибератак на российские промышленные предприятия связано как с социальной и экономической значимостью сектора, геополитической напряженностью, так и с особенностями технологического ландшафта. По мере цифровизации и увеличения связности ИТ- и ОТ-сегментов расширяется поверхность атаки, развитие инцидента все чаще затрагивает сразу несколько контуров. В этих условиях защита отдельных систем перестает быть достаточной, а ключевой задачей становится обеспечение киберустойчивости организации в целом.

Узнать больше
об исследованиях
Positive Technologies