Kaspersky ICS CERT

kaspersky

Киберугрозы для промышленных предприятий и OT-инфраструктур в 2025 году

Евгений Гончаров

29.01.2025 Версия 1.0

Глобальные процессы, меняющие ландшафт угроз

Охота за инновациями

Инновации с каждым годом все сильнее меняют нашу жизнь. Сегодня мир стоит на пороге очередной технической революции. Доступ к новым технологиям — билет в будущее, залог экономического процветания и политического суверенитета. Поэтому многие страны инвестируют в перспективные исследования и разработки в самых различных сферах — ИИ и машинное обучение, квантовые вычисления, оптическая электроника, новые материалы, новые источники энергии и типы двигателей, спутниковая связь и телекоммуникации, генетика, биотехнологии и медицина.

С точки зрения кибербезопасности интерес к инновациям означает, что APT-группы фокусируются на научных институтах и предприятиях, занимающихся передовыми исследованиями и разработкой. Поскольку спрос на технические ноу-хау растет, продвинутые злоумышленники из числа вымогателей и хактивистов также включаются в охоту за конфиденциальной информацией о новейших разработках.

Руководству промышленных предприятий следует помнить, что злоумышленникам может оказаться проще получить доступ к этой информации из технологической сети производственного объекта, чем из периметра исследовательской лаборатории или офисной сети организации. Цепочка поставок и сеть доверенных партнеров также являются очевидными потенциальными целями злоумышленников.

Искусственные ограничения и санкционные войны

Растущая геополитическая нестабильность, санкционные войны и новые искусственные барьеры, ограничивающие доступ к эффективным технологиям, создают искушение нарушать право интеллектуальной собственности мировых технологических лидеров. Это может привести к следующим рискам:

- Разработчики и поставщики OT-технологий столкнутся с тем, что существующие технические механизмы, встроенные в продукты, которые они поставляют своим клиентам, больше не гарантируют эффективную защиту их интеллектуальной собственности.

- Взломанные версии и нештатные модификации проприетарных продуктов, так же как и прочие решения для обхода лицензионных ограничений производителя, влекут за собой повышенные риски кибербезопасности, принося киберугрозы прямо внутрь технологического периметра.
- В дополнение к краже документации, связанной с передовыми технологическими наработками и новыми продуктами, злоумышленники продолжат охоту за техническими ноу-хау, собирая 3D-/физические модели и проекты CAD/CAM, как мы это видели в атаках Librarian Ghouls.
- Целью злоумышленников могут также стать и программы ПЛК, и SCADA-проекты, и прочие источники информации о технологическом процессе и алгоритмах управления оборудованием, хранящиеся в различном виде на различных устройствах внутри периметра технологической сети.

Новые технологии = новые риски информационной безопасности

Пробуя что-то совершенно новое, следует ожидать, что помимо обещанных преимуществ также возникнут неожиданные побочные эффекты с неизвестными последствиями. Сегодня многие промышленные предприятия идут в ногу с организациями из других секторов (например, финансового или розничной торговли) и внедряют IT-новшества, такие, например, как системы дополненной реальности и квантовые вычисления. Наибольший рост эффективности обещает, как и во многих других сферах, широкое использование систем машинного обучения и искусственного интеллекта, в том числе непосредственно на производстве — при управлении технологическим процессом. Уже сейчас применение таких систем на объектах, например, цветной металлургии может давать прирост выхода конечного продукта, оцениваемый десятками миллиардов рублей в год. Однажды ощутив такой прирост эффективности, предприятие уже не сможет отказаться от использования новой технологии, она законно становится важным производственным активом. Это может повлиять на ландшафт угроз несколькими путями:

- Неаккуратное использование технологий искусственного интеллекта в IT- и операционных процессах промышленных предприятий может привести к непреднамеренному раскрытию конфиденциальной информации (например, в результате попадания этой информации в обучающую базу модели) и появлению новых угроз безопасности, в том числе тех, которые на данный момент трудно предсказать.

- Как сами системы ИИ, развернутые на предприятии, так и уникальные данные, которые они используют (либо в форме сырых исторических данных телеметрии, используемых в качестве обучающей выборки, либо в форме включенных в модель ИИ весов нейронной сети), могут стать новыми целями для опасных кибератак. Например, если данные будут заблокированы или уничтожены злоумышленниками, их может быть попросту неоткуда восстановить. Кроме того, атака на ИИ-системы может не представлять угрозы функциональной безопасности для объекта-жертвы, то есть в отличие от традиционных OT-систем, они могут оказаться не такой уж рискованной целью для злоумышленников, чтобы держаться от них подальше.
- Злоумышленники также не игнорируют технический прогресс: использование ИИ на разных этапах подготовки и проведения атак — при разработке вредоносных инструментов и средств социальной инженерии (например, для генерации текста фишинговых писем) — снижает расходы и ускоряет тем самым развитие киберугроз. Эта тенденция определенно продолжится в 2025 году.

Проверенные временем технологии = новые риски информационной безопасности

Если систему не атаковали, это не значит, что она хорошо защищена. Возможно, до нее просто еще не добрались, ведь у злоумышленников были более простые, понятные и изученные пути решения их задач. Или вам просто везло.

Выражение «работает — не трожь» в технологических инфраструктурах промышленных предприятий приобретает особенный оттенок смысла и может означать, что система работает годами и даже десятилетиями без каких-либо модификаций, даже без установки критических исправлений безопасности и с исходной конфигурацией, включая неиспользуемые сетевые службы, отладочные интерфейсы и небезопасные пароли, — иногда с самого момента ввода в эксплуатацию.

Проблема осложняется порой низким качеством информации об уязвимостях в продуктах для OT, предоставляемой разработчиками и доступной из публичных источников. К счастью, злоумышленники пока крайне редко атакуют промышленные активы и системы промышленной автоматизации.

Однако помимо незащищенных систем промышленной автоматизации, таких как ПЛК и SCADA-серверы, безопасность которых на самом деле очень

сложно поддерживать, существует много типов устройств или целых инфраструктур, так или иначе связанных с технологической сетью, про безопасность которых просто забывают без объективных на то причин.

К таким устройствам и инфраструктурам, по нашему мнению, относятся:

- Телекоммуникационное оборудование. Его безопасность считается либо зоной ответственности оператора связи, либо чем-то вообще ненужным. Например, существует убеждение, что базовые станции мобильной связи и технологические сети мобильных операторов и без того достаточно защищены от кибератак, и поэтому «их никто не атакует». Каким-то странным образом эту проблему по большей части обходят стороной и исследователи безопасности. В то время как безопасность конечных устройств и их ключевых компонентов, например модемов, исследуется широко и глубоко, технических публикаций о результатах исследований безопасности базовых станций или оборудования для ядра сети до крайности мало. Тем не менее очевидно, что это оборудование может быть скомпрометировано, как минимум со стороны оператора, например, в процессе технического обслуживания. Да и сами телеком-операторы не то чтобы недосягаемы для кибератак, как нам показывает история про атаки Blackwood с использованием импланта NSPX30. Таким образом, стоит иметь в виду следующее:
    - Промышленным предприятиям никак нельзя исключать из модели угроз как минимум атаки типа «человек посередине» на телеком-оборудование и инфраструктуру операторов связи.
    - Учитывая скорость внедрения всевозможных умных систем удаленного мониторинга и управления, в первую очередь в сфере добычи полезных ископаемых и в логистике, но также и в прочих секторах, и на различных типах объектов, актуальность проблемы кибербезопасности инфраструктур, связанных с телекоммуникациями, со временем будет только расти. Так, для контроля безопасности труда в роботизированных инфраструктурах и при использовании на объекте автоматизированного транспорта мы наблюдаем повсеместное внедрение средств беспроводной связи. Очевидно, что промышленным предприятиям стоит инвестировать в их безопасность, чтобы избежать киберинцидентов, возможно, уже в 2025 году.
- Безопасность умных датчиков, счетчиков, оборудования для измерения и контроля и прочих устройств промышленного интернета вещей

традиционно находится на периферии внимания как использующих их предприятий, так и, закономерно, разработчиков. Тем не менее эти устройства, как показывает история FrostyGoop, попадают в поле зрения злоумышленников и становятся объектом атаки.

- Точки подключения мелких удаленных объектов промышленных инфраструктур, как правило, используют недорогое сетевое оборудование, иногда даже не рассчитанное на промышленное применение (например, устройства класса SOHO). Безопасность такого оборудования бывает крайне трудно поддерживать — как ввиду архитектурных ограничений, так и из-за сложности централизованного обслуживания. При этом злоумышленники могут использовать такие устройства не только для распространения вредоносного ПО «общего назначения» или для размещения агентов бот-сетей (как, например, в истории с Flax Typhoon/Raptor Train), но и в качестве точки проникновения в корпоративную или технологическую сеть промышленного предприятия.
- ОС семейства Windows на протяжении десятилетий является наиболее популярной платформой для рабочих станций и серверов систем автоматизации. Однако последние годы многие промышленные предприятия по разным причинам внедряют у себя в технологическом контуре все больше систем на основе ОС Linux. В некоторых случаях не последним аргументом в пользу выбора Linux является убежденность в том, что такие системы будут более устойчивы к кибератакам. С одной стороны, действительно, разнообразие вредоносного ПО для этой ОС не очень велико и вероятность случайного заражения ниже, чем в случае использования Windows. С другой стороны, защитить системы на базе Linux от целенаправленной атаки будет как минимум не проще, а в некоторых случаях — и сложнее. Дело в том, что:
    - Разработчикам защитных решений для Linux приходится догонять решения для Windows-инфраструктуры, ведь долгое время многие функции не были востребованы заказчиками и потому не были реализованы. При этом реализация новой функциональности для Linux обходится дороже — ведь приходится поддерживать великое множество параллельно развивающихся дистрибутивов ОС. Кроме того, интеграция решений безопасности не в приоритете у разработчиков ядра, поэтому, во-первых, не хватает эффективных штатных механизмов интеграции, а во-вторых, обновление ядра

может легко «сломать» совместимость, и простой пересборкой модулей при этом не обойтись.

- На стороне промышленных предприятий явно не хватает специалистов по информационной безопасности, достаточно хорошо разбирающихся в Linux, поэтому и безопасное конфигурирование устройств, и мониторинг и обнаружение инцидентов в системах на базе этой ОС могут быть недостаточно эффективны.
- Сами OT-решения под Linux и их разработчики часто демонстрируют недостаточную зрелость информационной безопасности и могут оказаться легкой целью для злоумышленников, как это выяснилось, например, при расследовании серии атак Sandworm на объекты критической инфраструктуры Украины.

Выбрал неправильно вендора — жди беды

Недостаточные инвестиции разработчиков или поставщиков технологий в собственную информационную безопасность — верный залог инцидентов у их клиентов. Проблема особенно актуальна для поставщиков нишевых продуктов и услуг. Один из показательных случаев — атака на CDK Global, приведшая к суммарным прямым потерям клиентов, превысившим миллиард долларов.

Ситуация для промышленных предприятий усложняется рядом факторов, наиболее важные из которых:

- Чрезвычайно длинные цепочки поставки технологий. Оборудование, в том числе системы автоматизации основных производственных активов, очень сложное. Парк промышленного оборудования предприятия может включать в себя как все основные компоненты, характерные для IT-систем, так и множество компонентов, созданных в результате кооперации большого количества производителей технологий, специфичных для промышленности. Многие из последних — это относительно небольшие производители нишевых решений, не располагающие ресурсами для обеспечения достаточного уровня информационной безопасности — своей и своих продуктов. Более того, подключение оборудования, первоначальная настройка и регулярное обслуживание почти всегда требуют специфических знаний — приходится задействовать специалистов из разных сторонних

организаций. Это, соответственно, увеличивает поверхность атаки на цепочку поставок и доверенных партнеров.

- Почти каждая крупная промышленная организация — сама себе вендор. Специфика отрасли и конкретного предприятия требует существенной доработки готовых и разработки новых решений автоматизации, уникальных для организации. Часто эти разработки ведутся либо внутри самой организации, либо руками дочерних или других родственных компаний. Все это множит почти все вышеописанные факторы риска — такие разработки редко ведутся на высоком уровне зрелости безопасности, а результирующие решения изобилуют простыми уязвимостями, доступными даже для не самых продвинутых злоумышленников. Естественно, эти проблемы уже используются в атаках и будут использоваться в дальнейшем.

Больше нельзя полагаться на сокрытие информации о работе промышленных систем

Доступность множества разнообразного инструментария для работы с промышленным оборудованием (просто посчитайте количество выложенных на GitHub библиотек и утилит, реализующих промышленные сетевые протоколы) делает разработку и проведение атаки на основные производственные активы промышленного предприятия многократно более простыми, чем еще несколько лет назад. К тому же и сами промышленные предприятия не стоят на месте — за несколько лет проделана большая работа не только по автоматизации производства, но и по инвентаризации и документированию систем и процессов. Теперь, чтобы добиться киберфизического эффекта на промышленном объекте, злоумышленникам больше не нужно читать учебники по проектированию систем противоаварийной защиты и привлекать внешних экспертов. Вся необходимая информация уже содержится в удобном электронном виде в офисной и технологической сети организации. Так, например, мы знаем случаи, когда злоумышленники в своих интервью рассказывают журналистам, что, попав в сеть предприятия, долго изучали документацию, описывающую системы и меры противоаварийной безопасности объекта, прежде чем выбрать системы автоматизации для атаки, — чтобы исключить риск угрозы для жизни сотрудников объекта и загрязнения окружающей среды в результате своих действий.

Центр реагирования на инциденты информационной безопасности промышленных инфраструктур «Лаборатории Касперского» (Kaspersky ICS CERT) — глобальный проект «Лаборатории Касперского», нацеленный на координацию действий производителей систем автоматизации, владельцев и операторов промышленных объектов, исследователей информационной безопасности при решении задач защиты промышленных предприятий и объектов критически важных инфраструктур.

Kaspersky ICS CERT ics-cert@kaspersky.com