АСУ ТП под давлением

Как меняется ландшафт угроз и архитектура защиты

Михаил ЯБЛОКОВ,
руководитель отдела по развитию продуктов InfoWatch ARMA

Кибервойна добралась до цехов и насосных станций: за последние годы АСУ ТП перестали быть далекой периферией и превратились в главный фронт атак. Хакеры бьют по уязвимым датчикам, ломают цепочки поставок и выводят из строя системы, на которых держится производство и энергетика. В этой статье – разбор, кто и зачем атакует промышленность сегодня, как меняется архитектура защиты и какие шаги помогут перейти от хаотичного тушения пожаров к предсказуемому управлению рисками.

Новая волна угроз: что изменилось с 2020-х годов

К началу 2020-х АСУ ТП окончательно вышли в первую линию киберпротивостояния. Если еще пять лет назад атаки на промышленные системы воспринимались как исключение из правил, сегодня это – предсказуемая закономерность. В 2024 г. в России зафиксирован рост количества киберинцидентов на 160% – почти в десять раз выше среднемирового темпа (17%). Причины – одновременное усложнение мотивов атакующих и рост цифровой экспансии в ИТ и ОТ-инфраструктуре. По данным InfoWatch, абсолютное количество инцидентов в России официально не раскрывается, однако открытые источники и базы инцидентов свидетельствуют об уверенной экспоненте.

Принципиально изменилась композиция атак: доминирующим вектором стала компрометация учетных данных, выросшая с 8% в 2020 г. до 20% в 2024-м. Одновременно выросла доля атак через уязвимые интернет-интерфейсы (с 5% до 13%) и через цепочку поставок (с 5% до 15%). Снижение демонстрируют фишинг (с 22% до 12%) и зараженные внешние носители (с 24% до 9%).

Новая тревожная тенденция – атаки на средства виртуализации и резервного копирования: злоумышленники целенаправленно шифруют виртуальные машины и уничтожают резервные образы, что блокирует сценарии восстановления и делает атаку крайне опасной.

Структура целей: кто и что под ударом

Инфраструктурная статистика подтверждает: наибольшую привлекательность для атакующих представляют инженерные рабочие станции (30%), SCADA-серверы (25%) и ПЛК (21%). Однако в последние два года наблюдается заметный рост атак на физический уровень: датчики, исполнительные механизмы, ЧМИ и удаленные терминальные блоки. Их объединяет общий знаменатель – слабая защищенность, отсутствие сегментации и невозможность развертывания защитных агентов.

Особую озабоченность вызывают устройства, расположенные

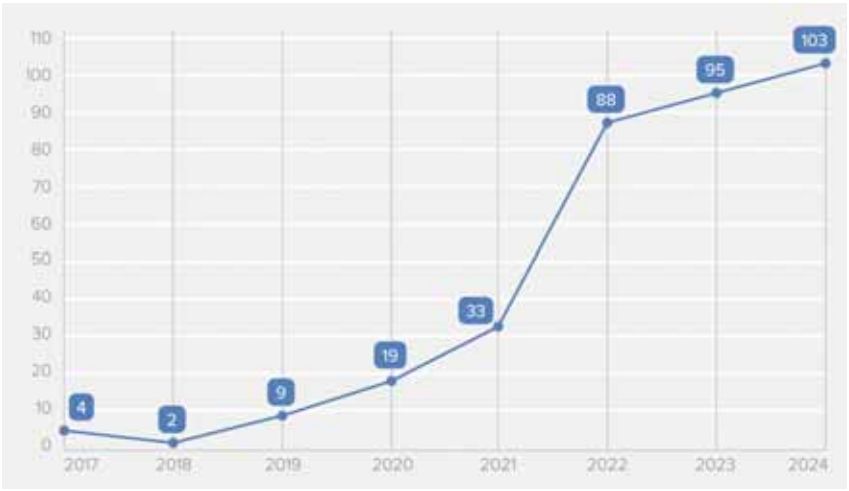

Рис. 1. *Количество киберинцидентов АСУ ТП в мире. Источник: ГК InfoWatch*

на удаленных площадках и подключенные по беспроводным каналам: риск многократно увеличивается в силу уязвимых протоколов и отсутствия контроля сетевых взаимодействий. Среда таких устройств зачастую не имеет обновлений, журналирования и может быть атакована без признаков инцидента на верхнем уровне.

Отчет InfoWatch демонстрирует расслоение между реальным риском и уровнем внимания к взлому: устройства уровня 0 (физические процессы) и 1 (базовый контроль) тестируются крайне редко, в то время как атаки на них фиксируются часто. Это создает опасную зону невидимости.

Эволюция мотивации атакующих группировок

2020–2024 гг. стали периодом переориентации мотиваций и типов акторов. Если в начале десятилетия подавляющее большинство угроз представляли APT-группировки (включая Incontroller, Xenotime, Dragonfly и др.), то к 2024 г. доминируют криминальные акторы. 73 инцидента в 2024 г. связаны с вымогательскими группами (например LockBit, BlackCat), 22 – с хактивистами, 8 – с APT. При этом многие APT-инциденты продолжают не попадать в публичную отчетность из-за их латентного характера.

Криминал эксплуатирует уязвимость процесса, а не уязвимость системы: атаки сочетают компрометацию VPN, горизонтальное продвижение (Lateral Movement) с помощью штатных инструментов (Living off the Land), разрушение резервных механизмов и вывод оборудования из строя. Отраслевой фокус – машиностроение, нефтехимия, фармацевтика.

Хактивисты используют аналогичные приемы, но цель – не выкуп, а дестабилизация. Резкий рост атак на энергетику (в том числе DER – распределенные энергетические ресурсы), транспорт и водоканалы совпадает по времени с международными политическими кризисами. Используются программы-вымогатели, DDoS, удаленное воздействие на системы релейной защиты и ЧМИ.

APT-группы сосредоточены на шпионских сценариях, подготовке диверсий и нарушении суверенитета. Их интерес – энергетика, оборонка, высокотехнологичные производства. Используются кастомные ВПО под SCADA, атакуется PNT (Positioning, Navigation, Timing), ядро диспетчерских систем.

Сдвиги в архитектуре защиты

На фоне усложнения атак эволюционируют и защитные стратегии. Согласно данным InfoWatch, в 2024 г. 65% компаний внедрили системы мониторинга OT-сети, 52% – решения по управлению уязвимостями, 46% – механизмы предотвращения угроз. Интенсивно внедряются EDR и NDR, особенно на уровнях 2–3 модели Purdue.

Рост получают также программно определяемые технологии сегментации, системы SOAR, анализ инвентаризации и применение Software Bill of Materials (SBOM). Сегментация становится не просто элементом архитектуры, а основой для управления потоком рисков: снижение числа связей между сегментами уменьшает поверхность атаки.

Внедрение Deception (технологий создания ловушек и приманок) пока ограничено, но отмечается как растущий тренд. Это ловушки, симуляторы активов, фальшивые среды, работающие на раннее выявление атакующего. Особенно востребованы в SOC и управлении инцидентами.

Нижние уровни Purdue защищаются плохо: устройства уровня 0 и 1 нередко находятся в одном домене с уровнями 3 и выше. Переход к защищенной иерархии, разнесенной по физике и логике, становится ключевым вызовом для архитекторов.

SOC для АСУ ТП остается редкостью: 12% компаний имеют выделенные центры. Однако совмещенный SOC (ИТ+ОТ) использует 36%, еще 20% полагаются на MSSP. Это говорит о нехватке зрелой модели мониторинга. При этом наблюдается рост активности по логированию событий из АСУ ТП: внедряются SIEM-коннекторы, собираются данные с устройств SCADA, ПЛК и инженерных станций.

Облака становятся важным элементом не только ИТ-, но и ОТ-ландшафта. В 2024 г. 35% компаний применяли облачные сервисы для аварийного восстановления, 30% – для размещения ЧМИ, 32% – для удаленного хранения исторических данных. Это требует пересмотра моделей доверия, оценки провайдеров и настройки защиты на стыках.

Технические и организационные приоритеты

Согласно прогнозам, к 2030 г. наиболее динамично будут расти:

- защита удаленного доступа (29%);
- управление рисками (28,3%) и уязвимостями (17,8%);
- внедрение СОВ (25,8%) и Deception (15%).

Переход от инфраструктурных закупок к зрелым системам управления – основной тренд. Инвестиции в NGFW и EDR сохраняются, но при этом набирают обороты SOAR, NDR, XDR, автоматизированные контрольные механизмы и средства анализа риска цепочек поставок.

Главными организационными барьерами остаются кадровый и организационный дефицит. 80% компаний фиксируют нехватку ИБ-специалистов. Только 50% внедрили программы повышения квалификации. Стратегии привлечения талантов (кадровый маркетинг, партнерство с вузами) реализованы менее чем у 35% компаний.

Требуется переход к системной зрелости:

- внедрение KPI и дашбордов ИБ;
- формирование риск-ориентированных моделей управления;
- контроль безопасности в цепочке поставок;
- сценарии восстановления, ориентированные на процессы.

Рис. 2. *Жизненный цикл технологий ИБ АСУ ТП. Источник: ГК InfoWatch*

Сдвиг происходит и в восприятии: ИБ из технического исполнителя становится интегратором устойчивости бизнеса.

Анализ рисков по уровням модели Purdue

Для оценки уязвимости инфраструктуры АСУ ТП и сопутствующих ИТ-систем удобно рассматривать архитектуру сквозного управления через призму уровней по модели Purdue. Она была разработана в 1990-х гг. и успешно применяется для структурирования уровней автоматизированных систем управления.

– **Уровень 5 (Интернет и внешние сервисы)** – самая уязвимая снаружи зона. Здесь актуальны риски веб-серверов, корпоративной почты и удаленных интерфейсов, особенно если осуществляется прямое подключение АСУ ТП к Интернету. Уровень защищенности крайне низкий, при этом активность атак очень высокая, включая постоянный фоновый скан и эксплуатацию типовых уязвимостей. Типовой вектор: компрометация внешнего веб-интерфейса удаленного администрирования и создание скрытого соединения с внешним сервером злоумышленника.
– **Уровень 4 (корпоративная сеть)** включает элементы ИТ-инфраструктуры, имеющие потенциальный доступ к ОТ. Основные угрозы – неправильно настроенные межсетевые экраны, уязвимые VPN, слабая сегментация сети и недостаточный контроль событий. Именно отсюда часто начинается проникновение в технологическую зону. Тестирование защищенности проводится на среднем уровне, атаки происходят регулярно, особенно через уязвимые каналы удаленного доступа. Типовой вектор: использование уязвимости в службе VPN для входа с украденными учетными данными и закрепление в системе.
– **Уровень 3.5 (демилитаризованная зона, DMZ)** – связующее звено между корпоративной ИТ-сетью и сегментом АСУ ТП. Здесь особенно критичны ошибки настройки шлюзов, неограниченный обмен данными, отсутствие ведения журналов и мониторинга. Хотя уровень защищенности формально выше, конфигурационные ошибки могут делать его уязвимым. Отсюда часто стартует горизонтальное перемещение злоумышленников (Lateral Movement). Типовой вектор: использование открытого порта промышленного протокола без аутентификации для туннелирования внутрь сегмента сети.
– **Уровень 3 (серверы и операционные системы SCADA)** – это ядро диспетчерского контроля, где обрабатываются команды и визуализируются процессы. Список угрозы включает в себя слабые механизмы контроля доступа, устаревшее ПО, отсутствие шифрования и неправильную реализацию RBAC. Здесь фиксируется множество атак, в том числе и целенаправленных. Уровень тестирования относительно высокий, но обычно все равно недостаточный. Типовой вектор: эксплуатация уязвимости в службе визуализации SCADA-панелей для выполнения произвольных команд.
– **Уровень 2 (верхний уровень управления)** включает диспетчерские интерфейсы, HMI, архиваторы и вспомогательные серверы. Основные риски – небезопасная передача данных, низкая осведомленность операторов, ошибки в конфигурации. Уровень защищенности и внимания – средний, при этом на этом уровне возможна точка воздействия на критически важные функции. Типовой вектор: загрузка модифицированного проекта HMI с вредоносным макросом через неподписанный источник обновлений.
– **Уровень 1 (ПЛК и базовый контроль)** – одна из наиболее уязвимых зон. Часто встречаются общие пароли, устаревшие

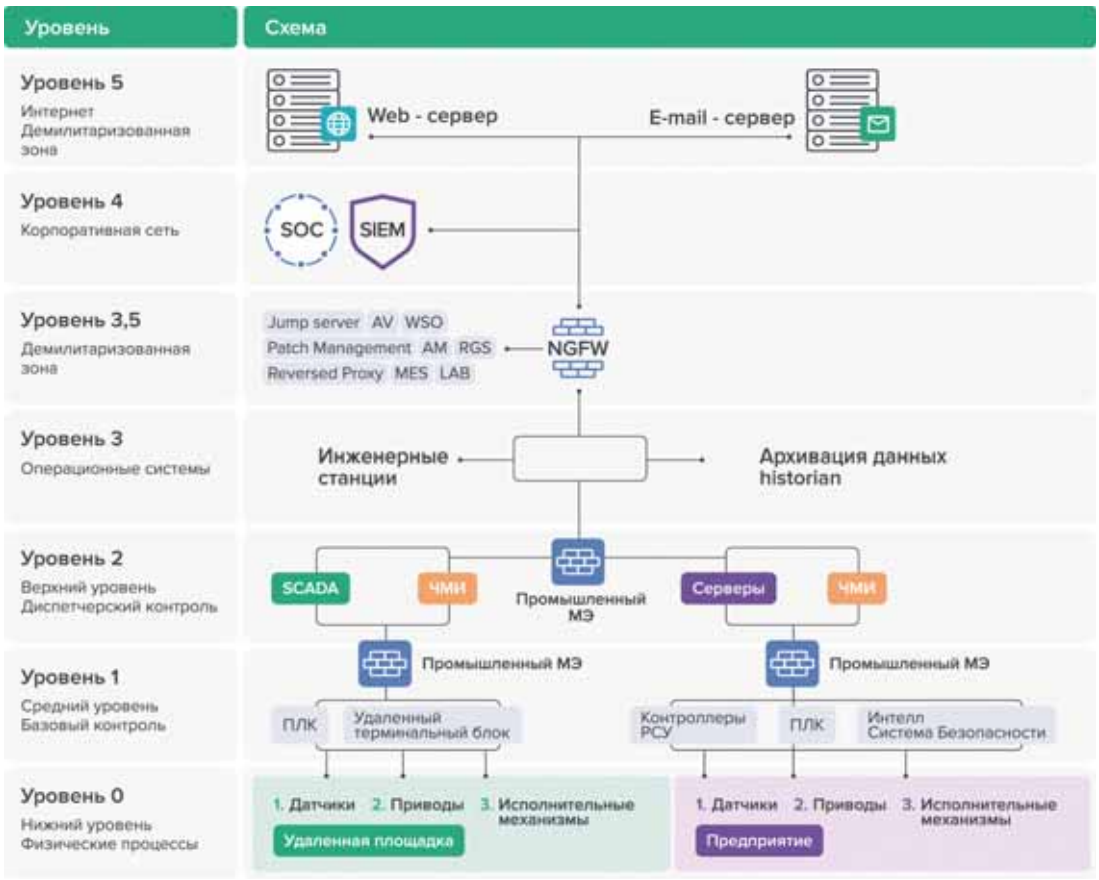

Рис. 3. *Модель Purdue. Источник: ГК InfoWatch*

прошивки, неуправляемые устройства, заражения через USB, небезопасные протоколы связи. Тестирование на проникновение практически не проводится. Атаки на этот уровень особенно эффективны на удаленных площадках, где отсутствует сегментация и наблюдение. Типовой вектор: передача вредоносной конфигурации на ПЛК через физический интерфейс или незащищенный инженерный порт.

– **Уровень 0 (физические процессы)** – самый низкий и наименее защищенный уровень. Характерны уязвимые прошивки, небезопасные конфигурации, встроенные пароли, открытые бэкдоры, слабые протоколы управления и отсутствие журналирования. Тестирование практически не ведется. На предприятиях этот уровень хоть как-то прикрыт, но на удаленных объектах он остается открытым для атак с минимальными усилиями. Типовой вектор: прямое управление физическим устройством через незащищенную шину управления (например без авторизации на Modbus TCP).

Такой многоуровневый анализ показывает важную асимметрию: нижние уровни системы – самые критичные для непрерывности производства, но в то же время наименее защищенные и наиболее уязвимые. Отсюда можно сделать важный вывод: стратегия защиты должна смещать фокус вниз по модели Purdue, усиливая изоляцию, наблюдаемость и контроль именно на нижних уровнях, где риск максимален, а уровень зрелости минимален.

Ориентиры на 2026 год

Ниже представлены уточненные и развернутые рекомендации для CISO, архитекторов безопасности и владельцев технологических процессов, которые хотят удерживать контроль над ИБ в условиях меняющейся угрозной модели:

1. Реинвентаризация ОТ-ландшафта

Провести полную ревизию технологической инфраструктуры:

- построить актуальный реестр всех устройств и компонентов АСУ ТП, включая безагентные и неуправляемые;
- категоризировать активы по уровню критичности к технологическим процессам (влияние на безопасность, непрерывность, финансы);
- выделить сегменты с устаревшим или неподдерживаемым ПО и невозможностью обновлений – приоритизировать замену, контейнеризацию, изоляцию;
- внедрить мониторинг даже на уровнях 0–1, используя пассивные сенсоры и зеркалирование трафика.

2. Сегментация по Purdue

Архитектурно и физически развести логические домены управления:

- минимизировать горизонтальные связи между уровнями 1–2 и 3+;
- внедрить промышленные NGFW на уровне 3.5 и шлюзы (диоды данных, прокси) для обмена между уровнями;
- интегрировать профилированные ACL и VLAN для каждой производственной зоны;
- устранить доверенные домены между ИТ и ОТ.

3. Расширение мониторинга и реагирования

Построить наблюдаемость и реактивные цепочки на события:

- развернуть NDR в демилитаризованных зонах и на уровне сбора телеметрии;
- использовать Deception в зонах управления и на удаленных площадках;
- обеспечить агрегацию логов с ПЛК, ЧМИ и SCADA через специализированные коннекторы в SIEM;
- применять поведенческий анализ и корреляцию событий, разделяя ИТ- и ОТ-логику;
- внедрить SOAR-платформу с преднастроенными плейбуками для технологических инцидентов.

4. Интеграция SOC с производственными процессами

Встраивать ИБ в оперативную логику работы объектов:

- пересмотреть SLA для реагирования на инциденты в производственном контуре (учет смен, ТПА, регламентов);
- обучить сменный персонал и диспетчеров распознаванию признаков кибератак;
- внедрить процедуру эскалации между ИТ-SOC и инженерными службами;
- обеспечить тестирование реагирования на инциденты в рамках реальных технологических сценариев (Red Team/Purple Team);
- реализовать резервные каналы управления с прицелом на киберустойчивость.

5. Развитие культуры устойчивости

Без участия персонала невозможно построить защищенную среду:

- внедрить программу обучения ИБ для всех категорий персонала, включая операторов, наладчиков и подрядчиков;
- интегрировать киберриски в систему управления операционными рисками;
- создать модель зрелости ИБ с визуализацией ключевых показателей;
- назначить ответственных за ИБ на каждом уровне производства и обеспечить им права для внедрения изменений;
- согласовать план Disaster Recovery не только на уровне ИТ, но и с учетом ОТ-сценариев, включая длительные простои и инциденты влияния на физические процессы.

Эти рекомендации – не абстрактные лучшие практики, а ответ на текущую угрозу, подкрепленные статистикой, динамикой инцидентов и поведением атакующих. Реализация хотя бы части из них позволит перевести защиту с уровня интуитивной реакции на уровень прогнозируемой и управляемой архитектуры безопасности.

От АСУ ТП к широкой категории АСУ

Существует еще один важный аспект. Проблематика защиты АСУ ТП не может более рассматриваться в изоляции от других видов автоматизированных систем, будь то информационная система предприятия, логистики, инженерной инфраструктуры или АСУ управления зданиями (BMS). Процессы цифровизации, унификации сетей и конвергенции ИТ/ОТ делают границы между этими категориями все более условными.

Во многих отраслях наблюдается эффект домино: компрометация АСУ ТП на производстве позволяет злоумышленнику с помощью бокового перемещения выйти на информационные системы бухгалтерии, снабжения или управления подрядчиками. С другой стороны, недостаточно защищенные корпоративные АСУ становятся точкой входа для проникновения в технологическую сеть. Классический пример – наличие общих доменов, недостаточная сегментация между ИТ и ОТ, единые учетные записи для систем диспетчеризации и ERP.

Особую уязвимость представляют собой так называемые гибридные АСУ: это, например, системы управления распределенной инфраструктурой (магистральный транспорт, сети связи, энергораспределение), где сочетаются SCADA-узлы, мобильные приложения диспетчеров, элементы CRM и внешние веб-интерфейсы.

К рекомендациям, изложенным выше в контексте АСУ ТП, должны быть добавлены уточнения для более широкой категории АСУ:

- любые АСУ, имеющие выход за периметр предприятия (подключение к ERP, CRM, аналитике, клиентским интерфейсам), должны управляться с учетом модели Zero Trust – с отдельными политиками доступа, логирования и анализа поведения пользователей;
- особенно в крупных холдингах и распределенных организациях необходимо четко понимать, какие АСУ связаны между собой, через какие протоколы и сервисы – и какая часть этого ландшафта видна системам мониторинга;
- раздельные команды ИТ и ОТ должны координироваться не только в рамках SOC, но и в части реагирования на сбои – например нарушение в BMS может стать прокси для атаки на энергетическую SCADA, а инцидент в системе управления логистикой – способом вывода из строя складской автоматизации.

Зрелая архитектура безопасности должна выходить за рамки производственного цеха. Она должна включать в себя всю инфраструктуру принятия решений и исполнения команд – от сенсора до корпоративного портала, от контроллера до цифрового двойника в облаке. Именно в такой парадигме и должна строиться стратегия безопасности АСУ в 2025 году и далее. ■