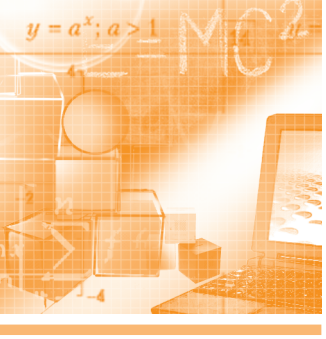

Не так страшен хакер, как собственный сотрудник: почему проекты ИБ упираются в человеческий фактор

Ильдар Галиев

Если спросить любого руководителя службы информационной безопасности (ИБ) крупного промышленного предприятия о самом сложном в его работе, он, скорее всего, вспомнит не компьютерный вирус и не хакерскую атаку. Гораздо чаще источником наибольшего напряжения становятся согласование технологических окон, взаимодействие со смежными подразделениями и риск остановки производства во время внедрения средств защиты. В проектах по обеспечению кибербезопасности автоматизированных систем управления технологическими процессами (АСУ ТП) технические задачи нередко оказываются проще организационных. Почему защита промышленных систем требует тонкого баланса между безопасностью и непрерывностью производства, какие проблемы возникают на практике и почему именно человеческий фактор зачастую определяет успех или провал проекта – об этом пойдёт речь в статье.

Непрерывность и стоимость простоев

В промышленности основным приоритетом является доступность и непрерывность работы технологических процессов. Потери от простоя оборудования оказываются астрономическими: по данным «Кросстеха», на простой приходится 50–70% всех убытков после киберинцидента, а всего одни сутки остановки крупного завода могут стоить сотни миллионов рублей. Поэтому правило «работает – не лезь» действует на предприятии повсеместно: любое вмешательство планируется с учётом рисков.

Обычно заказчики требуют представить детальный план работ с оценкой рисков и смягчающих мер. Например, если нужно установить защитное ПО на рабочую станцию оператора, в «Запросе на изменение» обязательно указывают последовательность действий, потенциальные проблемы (например, конфликт новой версии клиента с текущей ОС) и меры на случай сбоя (создание резервной копии системы для быстрого отката).

Чтобы сократить окна простоя, важно начинать работу с тщательного аудита АСУ ТП. Необходимо собрать точные данные об используемом оборудовании и программах (модели контроллеров, версии прошивок), сетевой топологии и промышленных протоколах (Modbus, Profinet, OPC и др.), а также о внешних связях (каналы связи между удалёнными площадками, удалённый доступ к оборудованию). Чем качественнее собрана информация на этапе аудита, тем меньше «сюрпризов» при внедрении. Например, одна из типичных накладок – это отсутствие питания там, где по чертежам оно было предусмотрено, и необходимость прокладки кабеля по всему серверному залу. Предварительное обследование позволяет такие ситуации минимизировать.

Ключевой приоритет проектов ИБ АСУ ТП – именно непрерывность работы технологических систем. На практике это означает, что большинство работ проводится в заранее согласованные «технологические окна» – часто это редкие плановые остановки оборудования (например, один раз в год на 2–3 дня) или ночные смены. Вне этих окон работы сводятся к минимуму. Для многих компаний такие окна – единственная возможность вмешаться в АСУ ТП, поэтому подготовка к ним требует месячной координации. Последовательность согласований может быть длительной: требуется направить официальные письма, заполнить унифицированные формы, предоставить копии документов (обычно за 1–2 недели до начала работ), а затем пройти вводный инструктаж по технике безопасности на территории заказчика и зачёт по его результатам. При этом каждый этап работ сопровождается чётким протоколированием и заранее согласованными мерами на случай непредвиденных ситуаций (резервные копии, «горячий» стенд для аварийного переключения и т.д.).

Организационные сложности и «конфликт интересов»

Проекты по защите АСУ ТП обладают повышенной организационной сложностью. С одной стороны, обычно участвуют службы ИБ и ИТ заказчика (как в классическом ИТ-проекте). Но к ним добавляются подразделения технологов, энергетиков, метрологов, а также операторы производства, мастерские и служба КИПиА. На практике это часто превращается в «кашу из интересов»: у каждой группы своя цель, бюджет и регламент работ. Поэтому на этапе подготовки проекта критически важно выяснить роль и степень участия всех сторон, а также границы их полномочий и зон ответственности. Например, необходимо обозначить:

- кто является ключевыми лицами и лицами, принимающими решения по проекту (должностные лица, оперативные дежурные, менеджеры, служба КИПиА и пр.);
- кто выступает держателем договора и спонсором бюджета (например, служба ИБ, ИТ или технологический департамент);
- регламент работы на объекте (время, когда разрешён доступ подрядчика на территории цехов, требования к сопровождению работ представителями заказчика);
- какие регуляторные или отраслевые требования применимы (например, необходимые сертификаты для ПО, методики проведения пусконаладки);
- необходимые средства индивидуальной защиты и разрешения (список СИЗ, оформление допусков в «чистые зоны», разрешение на привоз/вывоз оборудования).

На таких проектах подрядчикам приходится выступать профессиональными переговорщиками и психологами. Нередко на одном заводе приходится согласовывать действия не только с «главными» – директором и начальниками служб, но и убеждать средний менеджмент и сменных операторов. Иными словами, если руководство одобрило проект, ещё предстоит «достучаться» до сотрудников цехов и лабораторий. При этом в промышленном сегменте отчётливо проявляется один нюанс: «Отсутствие явных границ зон ответственности АСУ ТП, ИБ, ИТ, недостаточный уровень внутренних коммуникаций» – это массовые проблемы, мешающие слаженной работе. Специалисты отмечают, что часто определение зон ответственности и формализация обязанностей (выдача допуска, документирование процедур, чёткие инструкции) являются не менее важной задачей, чем техническая реализация.

В итоге успешный ИБ-проект требует не только внедрять технологии, но и «выстраивать коммуникацию» между всеми службами заказчика. Подрядчики заранее готовят блок-схемы взаимодействия, проводят переговоры и встречи с разными отделами. Цель – добиться понимания того, как изменения в АСУ ТП скажутся на работе каждого подразделения. Например, перед установкой нового межсетевого экрана обычно согласовывают с сетью участок подключения, с энергетиками – наличие ИБ-оборудования в шине электропитания, с автоматчиками – возможные задержки в командообмене. Такой подход резко снижает риски «неожиданного» конфликта интересов и помогает получить одобрение проекта «снизу вверх».

Условия и безопасность на объекте

Промышленные площадки предъявляют особые требования к подрядчикам, связанные с физической безопасностью и режимом объекта. Чаще всего речь идёт о заводах с огороженной территорией, контрольно-пропускным пунктом (КПП) и специальными зонами (производственными, газовыми, взрывоопасными и т.д.). В таких условиях требуется соблюдать целый комплекс мер.

- **Получение пропуска и инструктаж.** За пропуском в цеха подрядчику нужно обратиться заблаговременно: отправить заявление или письмо-запрос, заполнить требуемые анкеты (указать ФИО сотрудников, данные документов, сведения о технике), а затем пройти вводный инструктаж по охране труда и технике безопасности. Такие процедуры могут занимать от нескольких дней до недели. На КПП обычно проверяют документы, проводят медицинский осмотр (в некоторых случаях – дрожь лития) и проверку знаний по технике безопасности. Лишь после успешной проверки выдают нарукавные бейджи и полагающуюся экипировку. При этом доступ спецтехники (автобусов, грузовиков) также согласовывается заранее – иногда требуются разрешения на въезд транспорта и специальные удостоверения.
- **Разрешение на ввоз/вывоз оборудования.** На многих предприятиях запрещено выносить любой инструмент и технику без оформления через охрану. Если на выходе КПП обнаруживается неучтённый прибор или кабель, могут устроить досмотр и даже отправить специалистов на переделку бумаг. Поэтому до начала работ важно составить реестр вносимого оборудования: от ноутбуков и кабелей до съёмных носителей и сканеров штрихкодов. Каждую позицию следует внести в пропускные документы и отчитаться при выезде из цеха.
- **Средства индивидуальной защиты (СИЗ).** За исключением административно-бытовых помещений, сотрудникам запрещено появляться на территории производственных участков без СИЗ. Типичный комплект включает специальную одежду (спецкомбинезон или куртка с брюками из ткани без искрообразования), защитную обувь со стальным носком, каску, защитные очки и перчатки. В зонах с возможным задымлением или удушающими газами (так называемых «красных зонах») требуется иметь при себе самоспасатель–противогаз. За нарушение правил СИЗ сотрудник может быть не допущен к работе или отстранён от прохода на объект.
- **Дисциплина на территории.** Действуют строгие правила поведения: курение разрешено только в чётко обозначенных местах на улице или специальных «курилках», алкоголь полностью запрещён. Попытка пройти через КПП в состоянии опьянения может привести к инциденту: сотрудника отвозят на медосвидетельствование, блокируют пропуск и сообщают об этом в генподрядную организацию (что влечёт штрафы по договору).

Таким образом, работа на объектах АСУ ТП требует не только подготовки по ИБ, но и чёткого соблюдения заводских регламентов. Многие интеграторы включают в смету расходы на спецодежду, аренду транспорта для выезда в отдалённые цеха и обучающие материалы по технике безопасности. Знание этих требований заранее снижает риск задержек и штрафов во время проекта.

Долгосрочность и планирование проектов ИБ АСУ ТП

Проекты по информационной безопасности в АСУ ТП обычно растянуты

во времени. Специалисты отмечают: каждый этап комплексной ИБ-инициативы может занимать от полугода до 1,5–2 лет. В крупных производствах нет возможности «быстро захватить» все угрозы: работы планируются поэтапно, с приоритетом самых критичных площадок и устройств. При этом ждать окончания всего проекта, чтобы устранить известную уязвимость, часто бывает нельзя. На практике зачастую применяют стратегию «точечного закрытия пробелов» уже на ранних стадиях: параллельно с аудитом и проектированием начинают ставить базовые средства защиты – межсетевые экраны, антивирусные модули, системы контроля доступа. Такие меры хоть и не решают всех задач, но снижают риск простых атак без долгих согласований. Однако и после ввода первоначальных мер важно не останавливаться на «поставил и забыл»: непрерывный мониторинг, регулярное обновление конфигураций и поддержка 24×7 становятся нормой в отрасли.

Ключ к ускорению проекта – структурный и комплексный подход. Этап аудита должен выявлять реальные «точки доступа» в сеть АСУ ТП: какие контроллеры связаны с корпоративной сетью, какие каналы обмена не имеют шифрования, какие USB-порты остаются без контроля. На основе этого строят матрицу угроз и моделируют сценарии атак (например, вход из офиса через фишинговое письмо к базе управления технологией). Такой анализ позволяет определить реальные векторы проникновения и не сосредотачиваться на формальных рисках.

Кроме того, важно заключать соглашения с вендорами и проверять совместимость решений. В отличие от офисной ИТ, в промышленной технике часто встречаются устаревшие ОС и железо – контроллеры десятилетней давности, Windows XP на рабочих станциях, программы управления под редкими дистрибутивами Linux. Как отмечено в отраслевом обзоре, «ПО для ранее спроектированного АСУ ТП может функционировать только под Windows, начиная с XP. В таком случае возможности ОС ограничены, используются минимально допустимые требования, а заложенный резерв давно иссяк». Нельзя просто «накатить патч» или поменять драйвера, как на офисном компьютере. Часто решением будет создание отдельного тестового стенда или цифровой копии системы с целью проверки того, что защита не нарушит работу ПО. Многие компании на этапе подготовки проектируют пиринговые стенды с идентичным оборудованием, на которых прогоняют сценарии. Это особенно актуально при работе с импортозамещёнными устройствами: если русской SCADA-системе трудно добавить антивирус, решают задачу уровнями – например, изолируют хост в отдельной VLAN и усиливают сетевую сегментацию.

Итого, чем больше предварительных исследований и проработанных сценариев, тем меньше неожиданных задержек в процессе внедрения. «ИБ-проект АСУ ТП – это инвестиция во всё предприятие», – указывают эксперты. Стремление видеть «свет в конце туннеля» заставляет распределять работы и риски, а не тратить месяцы на неожиданности.

Логистика и удалённость объектов

Проектировщики ИБ-проектов должны учитывать и географические особенности промышленных предприятий. Большинство крупных заводов расположены за пределами городов (например, вблизи Урала, Сибири или на Севере) и занимают большие территории. Расстояние от административного здания до самого цеха нередко достигает нескольких километров. При планировании бюджета стоит заложить транспортные расходы и время на дорогу: как правило, завод не предоставляет машину для подрядчиков, приходится арендовать автомобиль или искать согласование на посадку в корпоративные автобусы.

Технологическая удалённость влияет и на формат работ. В сегменте АСУ ТП заказчики крайне редко предостав-

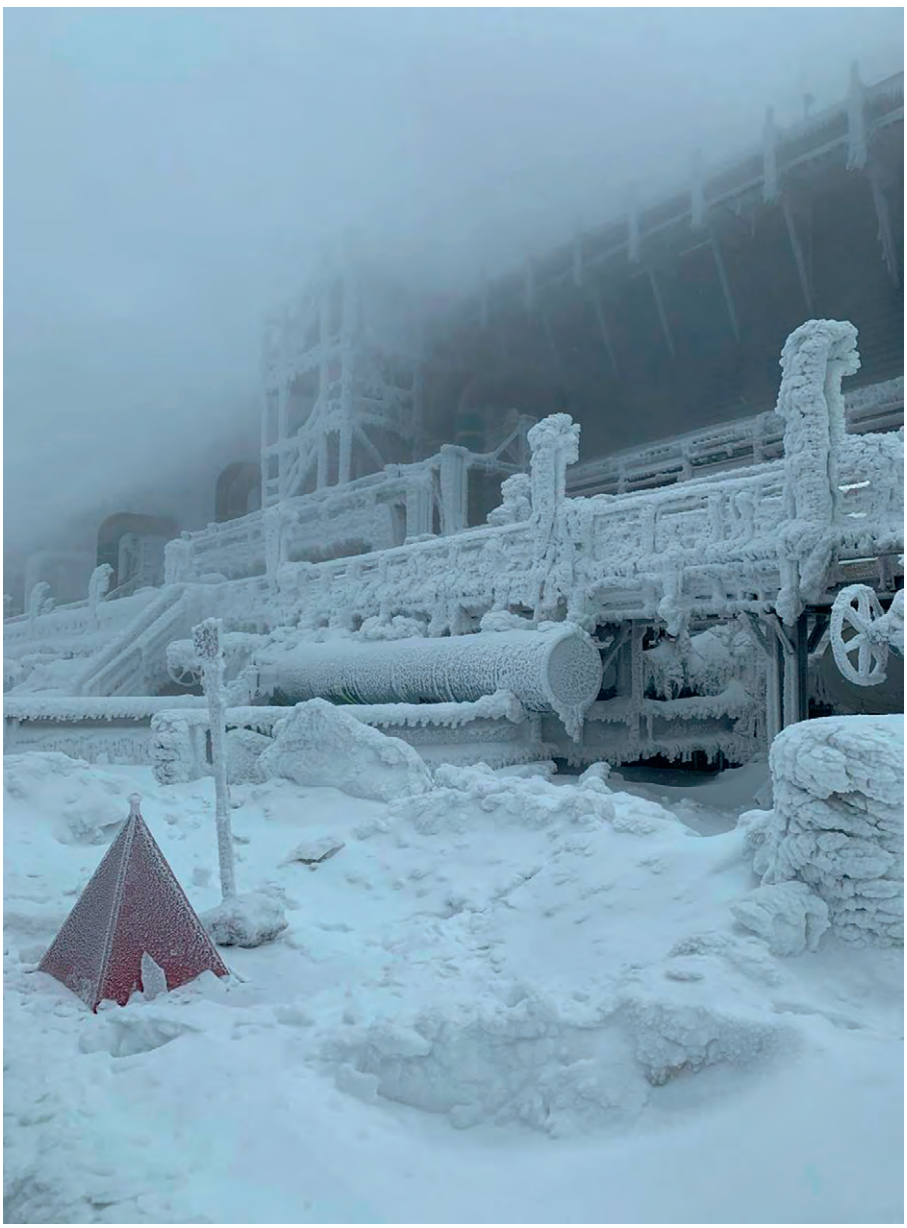

Рис. 1. Иногда приходится работать и в таких условиях

ляют постоянный удалённый доступ к системам: все настройки СЗИ (средств защиты информации) обычно выполняются на месте, в присутствии ответственных сотрудников заказчика. Только так компания может контролировать, чтобы после изменений производство заработало правильно. В ряде случаев подрядчики даже открывают филиалы в городах, близких к большим предприятиям–интеграторам, где регулярно требуются специалисты: так снижают затраты на выезды и добираются до «крупных клиентов», делая проектный сервис более устойчивым (рис. 1).

Отдельно стоит упомянуть ситуацию с производственными контрактами: на практике часто встречаются условия, обязывающие завод обеспечить удалённый канал связи для производителя оборудования (например, станков или турбин). Официально это нужно для мониторинга и поддержки, но на деле именно такой канал может стать лазейкой для злоумышленников. По оценкам практиков, потребность в «удалённом обслуживании» технологов становится одной из главных уязвимостей: несколько крупных инцидентов в России и мире были связаны с ошибками при удалённой перепрошивке оборудования со стороны вендоров. Эти случаи подтверждают, что любое внешнее подключение к АСУ ТП требует максимальной осторожности и избыточной аутентификации.

Технологические особенности промышленных систем

АСУ ТП – это «сборная солянка» старой и новой техники. На одном заводе могут соседствовать контроллеры Siemens начала 2000-х (или даже 90-х годов), рабочие станции на Windows XP, а также современные SCADA и MES-системы. Из-за этого стандартные подходы информационной безопасности часто не работают. Например, обычная практика – обновить драйверы или ОС – в промышленных контроллерах бессмысленна: смена оборудования производится раз в 15–20 лет. Даже сертифицированные отечественные решения могут «не вытягивать» по производительности или не поддерживать старые протоколы.

В таких условиях интеграторы применяют гибкие схемы: накладывают виртуальную среду или специальные прокси-серверы, используют сетевую сегментацию по зонам (например, «Интернет → офисная сеть → DMZ → промышленная сеть»), ограничивают каналы доступа до строго необходимых. Если встроенные механизмы защиты ОС недоступны (как отмечено в литературе, «зарезервированные ресурсы иссякли», и полноценно поставить только дополнительные средства НСД не получится), то усиливают меры «физической безопасности» и сетевого контроля: ставят контролируемые терминалы, ведут журналирование действий, разбивают процесс на отдельные зоны и прозрачно мониторят трафик (анализ отклонений в коммуникациях часто даёт раннее обнаружение атаки).

Наконец, при работе с устаревшим ПО часто приходится балансировать на грани допустимого. Порой единственный выход – оставить старую систему без изменений и усилить смежные технологии: например, вместо сложной модернизации блока использовать промышленный файервол, который позволит фильтровать команды между сегментами.

Всё это требует от интегратора творчества: каждый проект ИБ АСУ ТП, по сути, уникален и собирается «из набора имеющихся инструментов», при этом нельзя навредить основному производству.

Осведомлённость и обучение персонала

Нередко столкновение «мира ИБ» и «мира технологов» сопровождается непониманием и сопротивлением. Инженерам и операторам АСУ ТП не до конца ясна логика мер по безопасности: почему для доступа к пульту управления вводят сложные пароли и двухфакторную авторизацию?

Поэтому важный этап любого проекта – повышение осведомлённости сотрудников АСУ ТП.

Реализация этой задачи обычно включает разработку понятных инструкций пользователя и администратора систем безопасности, обучающие сессии и демонстрации. Например, проводят тренировки по реагированию на инцидент: оператору показывают, как срабатывает IDS/IPS при попытке несанкционированного подключения к контроллеру или визуализацию событий в SIEM-системе, и объясняют, как это связано с показателями процесса. Такие живые примеры (не «меняйте пароли раз в три месяца, потому что надо»!) демонстрируют причину и эффект мер ИБ.

Кроме того, налаживают обратную связь: ответственные специалисты АСУ ТП часто вовлекаются в работу команды ИБ. Это может быть совместная работа над тестированием решений, круглые столы или участие в отраслевых мероприятиях. Приглашение представителей производства на конференции по ИБ АСУ ТП (например, «ИБ-КВО» или «ЦИПР») и участие ИБ-специалистов в профильных выставках (ИБ-Технологии, «Съезд метрологов» и др.) укрепляет взаимопонимание. В конечном счёте цель одна – заложить в рабочую культуру предприятия понимание того, что информационная безопасность – это не лишь «дополнительная головная боль», а гарантия стабильности производства.

Заключение

Проекты ИБ в АСУ ТП – это особый мир со своими правилами. Ключевой вывод практиков: многие сложности связаны не с технологиями, а с организацией и человеческим фактором. Для их преодоления интеграторы должны быть «готовы ко всему»: иметь в штате инженеров, разбирающихся и в ИТ, и в промышленных технологиях, уметь выстраивать диалог с разными департаментами и учитывать жёсткие регламенты заказчика. Взамен они получают большие возможности: промышленность активно инвестирует в кибербезопасность своих объектов, а знания и опыт работы в АСУ ТП становятся важным конкурентным преимуществом. По словам экспертов, отрасли с наибольшими потерями от простоев – это именно промышленность, транспорт и энергетика. Значит, адаптация решений ИБ под особенности АСУ ТП – гарантия того, что проект будет востребован и принесёт реальную пользу. Все эти нюансы делают любые ИБ-инициативы на производстве долгосрочными, требующими тщательной подготовки, но взамен обеспечивают максимальную эффективность защиты критичных систем. ●

Литература

1. Отраслевые исследования и обзоры рынка информационной безопасности АСУ ТП, практические рекомендации экспертов.

Автор – руководитель направления «Развитие услуг» компании «Кросстех»