Безопасность АСУ ТП глазами аудитора

Максим ДОБРЯКОВ,
руководитель Отдела консалтинга и аудита, АО «ЭЛВИС-ПЛЮС»

Обеспечение информационной безопасности АСУ ТП на промышленном предприятии – одна из наиболее актуальных задач. Выход системы из строя или даже нештатная ее работа может привести к катастрофическим последствиям. Особая роль в профилактике сбоев отводится подготовке и проведению внутренних и внешних аудитов безопасности АСУ ТП. На что следует обратить внимание, чтобы избежать досадных ошибок, допускаемых не только начинающими аудиторами?

Отраслевые приоритеты

Как показывает опыт нашей компании, соблюдение конфиденциальности в АСУ ТП – не первоочередная задача, как, например, в корпоративных системах и сетях. А вот обеспечение целостности и доступности – основа бесперебойного функционирования АСУ ТП. Функциональная безопасность АСУ ТП – необходимое условие для того, чтобы не допустить сбоев технологического процесса.

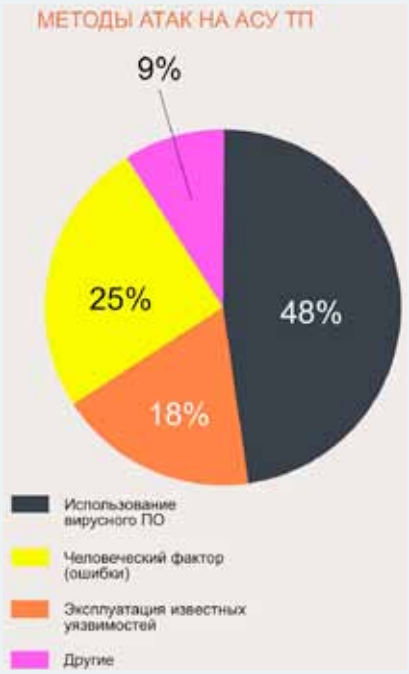
В то же время стоит отметить, что обеспечение конфиденциальности на промышленных предприятиях требуется в бизнес-системах, коммерческих системах учета СИКН, весовых системах и подобных им.

Киберугрозы в цифрах и фактах

Статистика угроз информационной безопасности только ухудшается. Промышленные предприятия в РФ подвергались кибератакам в 12% случаев от общего числа происшествий в 2024 г. (в этом списке выше только ритейл: 15%). Обращает на себя внимание тот факт, что хакерским атакам подвергаются все секторы российской экономики.

По традиции использование вредоносного ПО, а именно вирусов-вымогателей, вирусов-шпионов и ПО для удаленного управления, служит основным способом совершения атак на промышленную инфраструктуру и составляет около половины всех случаев. Далее идут атаки, связанные с эксплуатацией известных уязвимостей инфраструктуры АСУ ТП, и, конечно, человеческий фактор.

Понимание рисков, связанных с безопасностью АСУ ТП, для большинства пришло наконец с появлением 187-ФЗ, утвердившего требования к защите объектов КИИ, к которым относятся почти все АСУ ТП. Конкретные потенциальные риски, последствия от реализации компьютерных



инцидентов на объектах КИИ указаны в Постановлении Правительства № 127, утвержденном во исполнение указанного Федерального закона. Новые требования устанавливают виды возможного ущерба конкретным предприятиям и РФ из-за компьютерных инцидентов, которые могут возникнуть на таких объектах.

Подготовительный этап

Не стоит лишний раз говорить о важности аудита, расскажу, как мы готовимся к его проведению. Во-первых, необходимо составить методику проведения аудита согласно ТЗ и действующему законодательству, опыту, использовать лучшие практики. Во-вторых, подготовить чек-листы аудита, содержащие оцениваемые требования. В-третьих, согласовать свои работы непосредственно с сотрудниками предприятия, составить совместно с ними матрицу коммуникаций и утвердить план проведения аудита. По структуре план аудита может быть хоть почасовым.

В рамках аудита ИБ АСУ ТП мы работаем с администраторами и инженерами АСУ ТП (они «цари и боги АСУ ТП», а в рамках таких систем и администраторы, и сетевики, и прикладники, и разработчики), технологами (для оценки критичности автоматизируемых процессов), специалистами по ИБ предприятия (в рамках общей оценки безопасности), администраторами сети (если АСУ ТП взаимодействует с внешними сетями), операторами АСУ ТП (обычно общаемся с ними, чтобы выяснить информацию, которую пытаются скрыть инженеры), изредка даже с разработчиками (для получения дополнительных сведений).

Так, во время аудита оператор АСУ ТП, работая «в режиме киоска» сам показал мне, как свернуть SCADA несколькими способами без ввода пароля администратора, хотя администратор клятвенно уверял, что это невозможно. Естественно, там же, на месте, оператору за это «влетело». По опыту скажу, что способов выхода из «режима киоска» достаточно много, и мы их стараемся изучать до аудита или во время проведения.

Технология проверки

Непосредственно в рамках работ проводится технический аудит ОС и SCADA на АРМ и серверах, HMI-панелях, на станках с ЧПУ, на программаторах, а также собираются и анализируются настройки сетевого оборудования. Наши специалисты оценивают, как реализована физическая безопасность, изучают организационные меры по ИБ.

По безопасности ПЛК стоит пояснить, что обычно смотрим «руками» инженера АСУ, но, как правило, не лезем, а в проекте АСУ ТП изучаем возможности внутренних механизмов безопасности ПЛК, а также документацию.

Нельзя не коснуться темы, как обычно организована защита АСУ ТП на промышленном предприятии. Как уже отмечалось, упор делается на функциональную безопасность, противоаварийную защиту, механические блокировки, релейную автоматику, а также на резервирование технических средств (в частности, ПЛК). Как правило, на высоком уровне реализована физическая безопасность промышленных объектов, что связано не только с пресловутым контролем за «несунами», но и зачастую продиктовано антитеррористическими требованиями.

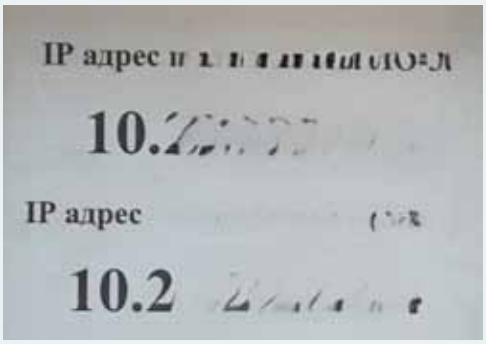
Что касается технических мер ИБ, реализованных на АСУ ТП, почти всегда выполняются процедуры резервного копирования, реже – используются средства антивирусной защиты и ограничения программной среды для оператора.

Слабые звенья безопасности

Рассмотрим основные недостатки, которые наши специалисты обнаруживают во время аудита:

- отсутствие самых базовых мер безопасности, таких как парольная защита, регистрация событий безопасности, отсутствие процедур внутреннего контроля и инвентаризации активов;
- отсутствие процессов управления логическим доступом, учетными записями;
- наличие нелицензионного ПО, в том числе ПО средств защиты;
- отсутствие обеспечения сетевой безопасности (при наличии взаимодействия с внешними сетями);
- неконтролируемый/нелегитимный удаленный доступ;
- наличие нелегитимных беспроводных соединений.

На фото – обнаруженная нами наклейка около администраторской машины с IP-адресами серверов АСУ ТП и ниже к ним – пароли



от ОС и от SCADA WinCC. Причем логины и пароли были идентичны для всех серверов. Стоит также заметить, что это были не локальные системы.

Кроме того, наши специалисты обычно выявляют:

- устаревшее ПО и оборудование, невозможность его замены, сложности с импортозамещением;
- отсутствие сопровождения со стороны разработчика, инженеры АСУ ТП сами меняют проекты «на коленке»;
- неподобающие условия содержания ТС;
- устаревшую документацию на АСУ ТП или ее отсутствие;
- отсутствие ограничения на использование USB-портов;
- отсутствие или незнание требований по информационной безопасности.

Например, есть риск «погасить» работающую SCADA на два часа и более просто при вызове журнала «алертов», если она установлена на устаревшем оборудовании или на недостаточно производительных машинах. Не приходится говорить о том, чтобы установить просто антивирус на таком оборудовании.

Из-за отсутствия должного понимания необходимости обеспечения защиты АСУ ТП возникает потребность в аудите ИБ таких систем и сложности в его проведении неизбежны. Типовые примеры, с которыми мы как интегратор ИБ сталкиваемся на практике:

- проведение работ только в технологические «окна», что создает большие проблемы с планированием;
- незнание персоналом своего оборудования;
- отсутствие необходимых людей на месте;
- HMI-панели не относятся к АСУ ТП;
- станки с ЧПУ не являются объектами защиты;
- ситуация «не ждали»;
- слабые вычислительные мощности не позволяют физически провести аудит, не запускаются настройки;
- страх работников, просят не наказывать и т. д., просят не «светить» результаты аудита, просят денег от руководства.

Уровень сопротивления

Отдельно стоит сказать о противодействии со стороны персонала АСУ ТП на местах. Чаще всего работники думают, что их после аудита накажут или уволят, реже они делают это из вредности. Вот, например, что мы нередко встречаем:

- сокрытие и отрицание отдельных компонентов АСУ ТП или даже системы целиком;
- отрицание наличия подключений к внешним сетям, наличия средств удаленного и беспроводного доступа;
- именование АСУ ТП системами мониторинга, чтобы утаить критичность системы;
- отсутствие заинтересованности;
- конфликт со специалистами в сфере ИТ и ИБ предприятия;
- отказ в сотрудничестве в проведении аудита.

В июле 2022 г. в ходе аудита объектов КИИ в интересах одного из наших министерств я обнаружил в цеху неучтенный и скрытый от министерства итальянский станок с ЧПУ. Более того, к нему удаленно были подключены программисты из Италии, на тот момент уже недружественной страны, и дорабатывали код после аварии. Правда, проводилось это под контролем инженеров онлайн.

В ответ на вопрос «почему?» мне пояснили, что станок критичный для производства, а если сообщить о нем министерству, то его могут запретить использовать. Эта история о том, что нужно искать золотую середину: безопасность не должна мешать производству, но и риски пренебрежения кибербезопасностью крайне высоки.

Ценность аудита

Нельзя не разъяснить, для чего процедура, если и так все работает. Внешний аудит ИБ как минимум позволяет провести:

- инвентаризацию активов;
- оценить эффективность применяемых средств и мер защиты информации, а также получить рекомендации по их модернизации;
- понять характеристики и компоненты АСУ ТП, которые влияют на уровень защищенности;
- получить внешнюю независимую оценку;
- оценить соответствие требованиям законодательства.

Вместо заключения

Наш опыт наблюдений за тенденциями развития ИБ АСУ ТП в последние годы позволяет сделать следующие выводы. Появилось понимание необходимости защиты АСУ ТП. Как правило, закреплена ответственность за отсутствие обеспечения безопасности АСУ ТП и определены сферы использования таких систем, критичные для государства. Предприятия стали проводить аудиты ИБ. В штатном расписании большинства крупных промышленных предприятий есть специалист по информационной безопасности. На производственных площадках начали проводить киберучения и создавать цифровые двойники. ■