Где кроются реальные проблемы защиты АСУ ТП?

Владимир Акименко, *руководитель Центра кибербезопасности критических инфраструктур АО "ЭЛВИС-ПЛЮС"*

Важность вопроса защиты АСУ ТП

Часто под управлением технологическими процессами подразумевают некую замкнутую производственную систему. Считалось, что технологические сети и системы изолированы от внешнего мира, поэтому обеспечение информационной безопасности (ИБ) в этой сфере не признавалось актуальным. Однако в последнее время стала наблюдаться активизация со стороны киберсообщества, которая проявляется в форме кибертерроризма, информационного шпионажа и даже шантажа.

Кроме того, вследствие повышения доступности средств и инструментов удаленного влияния на информационную инфраструктуру совершенствуются методы коммерческого информационного воровства и мошенничества. Существуют реальные примеры, когда происходят умышленные изменения производственных показателей за счет того, что данные в автоматизированной системе управления технологическим процессом (АСУ ТП) доступны для модификации.

Тем не менее руководство промышленных предприятий и персонал АСУ ТП недостаточно осведомлены в вопросах обеспечения ИБ и часто недооценивают важность решения задач защиты информации. Поэтому зачастую заказчики в лучшем случае пытаются перенести технологии защиты "офисных" информационных систем на технологическую инфраструктуру и АСУ ТП, что далеко не всегда целесообразно и эффективно.

В то же время государство уделяет большое внимание вопросам организации защиты АСУ ТП и других управляющих и информационных систем критически важных и потенциально-опасных объектов. В соответствии с государственной политикой в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов (КВО) разрабатываются нормативно-правовые акты о безопасности на критически важных, потенциально опасных объектах и объектах критической информационной инфраструктуры Российской Федерации.

Эти документы существенным образом меняют взгляд на порядок проведения работ и принципы технической реализации систем защиты информации. Ценность данных документов состоит даже не в том, что они определяют какие-то конкретные требования к мерам защиты, а в том, что они вносят определенность в подходы и шаги по обеспечению защиты. Однако это требует определенных знаний, понимания и навыков в данной области у заказчиков. Последовательность политики государства в этой сфере также вынуждает их более серьезно и внимательно подходить к вопросам защиты информации. Кроме того, нужно понимать, что реализация мер защиты по нормативным требованиям подразумевает проведение квалифицированной объективной оценки защищенности эксплуатируемых АСУ ТП и высокого уровня экспертизы при внедрении систем защиты, поскольку необходимо учитывать не только функциональные возможности внедряемых средств защиты информации, но также особенности и ограничения используемых технологий АСУ ТП и иных информационных систем КВО и объектов критической информационной инфраструктуры (КИИ).

Необходимость обеспечения безопасности АСУ ТП и объектов КИИ обусловлена и ужесточающимися требованиями законодательства. Согласно новым нормативно-правовым актам за нарушение законодательства о безопасности критической информационной инфраструктуры наравне с дисциплинарной, гражданско-правовой и административной будет предусмотрена уголовная ответственность.

Подытоживая, важно отметить, что обеспечение безопасности информации – не самоцель, а один из инструментов, используемых для обеспечения бесперебойной и штатной работы АСУ ТП, что в свою очередь позволяет гарантировать промышленную безопасность объектов, управляемых АСУ ТП. Кроме того, система защиты информации дает возможность решать вопросы экономической безопасности за счет исключения изменения учетных данных, запрета нелегального доступа, предотвращения возможности несанкционированного искажения данных.

Все вышеизложенное, а также растущая зависимость управляемого технологического процесса от устойчивой и бесперебойной работы АСУ ТП говорит о высокой степени актуальности вопроса защиты АСУ ТП.

Основные этапы создания систем защиты АСУ ТП и сопутствующие проблемы

Для удобства процесс создания систем защиты (СЗ) АСУ ТП можно условно разделить на четыре стадии. Рассмотрим каждую из них, а также проблемы, которые возникают на этих стадиях.

1. Обследование и аудит

Для бизнеса важно, чтобы каждая инвестиция была обоснована. Уже на начальном этапе создания системы защиты АСУ ТП выясняется, что часто заказчики не представляют себе реальное устройство технологического процесса. Отсутствует связка между различными участками технологического процесса, обнаруживаются проблемы с инвентаризацией и определением самого объекта защиты и его границ. Самое опасное, что многие заказчики не осознают существование этой проблемы.

Поэтому специалисты ЭЛВИС-ПЛЮС убеждены, что создание систем защиты АСУ ТП необходимо всегда начинать с аудита. Причем необходимо понимать и принимать в расчет, что данный процесс, как и само создание системы защиты, в большинстве случаев проходят на действующих предприятиях без остановки технологических процессов и без отрыва обслуживающего персонала от работы.

Важной постановочной частью работ по созданию СЗ АСУ ТП может стать экспресс-аудит, выполнение которого сотрудниками ЭЛВИС-ПЛЮС не потребует много времени и обработки большого объема исходных данных; большей частью он может проходить в форме интервьюирования. Выполнение этих работ покажет заказчику общую картину состояния ИБ в технологических системах и позволит определить основные проблемы и направления решения задач защиты информации в критичных технологических системах организации или промышленного предприятия.

2. "Артподготовка"

Итак, руководство понимает всю важность и необходимость создания системы защиты АСУ ТП. Проведен аудит и выявлены объекты защиты. Далее начинается работа с технологами, так как никто лучше них не понимает, как устроены технологические процессы на предприятии. И здесь вступает в игру человеческий фактор. Не понимая всей сути задачи, целей и содержания работ, сотрудники на местах начинают тормозить процесс создания системы защиты АСУ ТП, а порой и саботируют его.

Для того чтобы этого не происходило, необходимо провести полномасштабную подготовку всего персонала, вовлеченного в процесс, донести необходимость и обоснование создания комплексной системы защиты до специалистов заказчика на всех уровнях, используя все доступные средства вплоть до выпуска соответствующих приказов о назначении ответственных.

3. Оценка ущерба

После проведения аудита, определения объектов защиты и моделирования угроз возникает задача по материальной оценке возможного ущерба. Экономический ущерб определяется на основании цепочки: "угрозы – нарушения – последствия – ущерб". В идеале последствия должны определять технологи, а денежный эквивалент ущерба должны оценивать специализированные организации, владеющие соответствующими методиками. Но в декларациях промышленной безопасности, которые нам встречались вплоть до настоящего времени, совершенно отсутствуют проблемы и риски, связанные с нарушением работы АСУ ТП. Отсутствие доступного методического аппарата, позволяющего квалифицированно оценить степень ущерба от нарушений в работе АСУ ТП, усложняет процесс оценки ущерба. Применение экспертных оценок неподготовленного персонала может приводить к ошибочному повышению уровня требований и, как следствие, усложнению и удорожанию СЗ. Пока эта проблема не решена, данный вопрос приходится решать интеграторам в плотном взаимодействии с соответствующими службами заказчика.

4. Применение решений защиты АСУ ТП

Наконец мы дошли до этапа реализации системы защиты АСУ ТП, где также существует своя специфика.

Во-первых, это определенная статичность системы, которая не позволяет использовать классические средства адаптивной защиты (антивирусные средства с режимом эвристического анализа, средства предотвращения атак и т.п.). То же касается и межсетевых экранов: в АСУ ТП используются свои протоколы, и обычный межсетевой экран зачастую просто бесполезен. Такие условия приводят нас к необходимости использования специализированных систем обнаружения вторжений. При этом обычные режимы систем предотвращения вторжений (IPS) не подходят для защиты АСУ ТП, потому что существуют большие риски блокирования работы системы и влияния на техпроцессы.

Во-вторых, отсутствует наработанная база инцидентов, как, например, в классических антивирусах. Большинство целенаправленных угроз, связанных с нарушением безопасности АСУ ТП, сравнительно недавние. Промышленные системы изолированы от публичного доступа и, в отличие от интернет-систем, где информация о нарушениях или атаках становится доступна и известна тут же всему мировому сообществу, как правило, ограничивается локальными инцидентами. Кроме того, каждая информационная система АСУ ТП специфична. К примеру, даже если мы говорим про одну и ту же технологическую установку подготовки нефти, но построенную на базе средств различных производителей, она может иметь разную архитектуру, разные протоколы, разные датчики, разные параметры контроля технологического процесса. Поэтому в случае с АСУ ТП все специфическое вредоносное программное обеспечение (ПО) и угрозы, как правило, узконаправленные.

Кроме того, проведение работ по созданию СЗ АСУ ТП дополнительно осложняется такими факторами как:

- отсутствие организованного взаимодействия технологической службы, подразделения информатизации и службы ИБ;
- отсутствие сведений и понимания эксплуатирующего персонала о работе АСУ ТП на уровне информационных потоков, протоколов, данных;
- использование устаревшего оборудования, отсутствие поддержки, обновлений, описаний, применение проприетарных протоколов, недокументированность, отсутствие документации в электронном виде, часто устаревшая и неактуальная документация;
- при проведении аудита и работ по созданию СЗ АСУ ТП часто обходят стороной рассмотрение систем противоаварийной защиты (ПАЗ), которые также могут содержать уязвимости и являться объектом атак.

Проблемы, подобные описанным выше, возникали и на заре становления отрасли коммерческой информационной безопасности, когда вопросы обеспечения ИБ пытались решать отдельно от ИТ. Сейчас же многие проблемы в этой области снимаются из-за более плотного взаимодействия специалистов ИТ и ИБ, решающих совместно задачи обеспечения ИБ-ресурсов информационных систем организаций. Ожидается, что аналогичные проблемы будут возникать и при реализации систем защиты объектов критической информационной инфраструктуры (КИИ), усиленные сложностью, связанной с необходимостью построения комплексных систем защиты, затрагивающих элементы различных по назначению, областям применения, архитектуре, составу защищаемых ресурсов, их категорий и условий эксплуатации систем.

Специфика выбора решения для защиты АСУ ТП

Каждая АСУ ТП построена на базе какого-то конкретного производителя, у которого есть свои требования, условия, а у многих вендоров решений по АСУ ТП есть и рекомендации, в том числе по обеспечению информационной безопасности. И в этих рекомендациях, в частности, присутствуют требования по продуктам или по средствам, которые должны быть использованы для защиты АСУ ТП, вплоть до конкретных релизов программного обеспечения. В этом случае ни заказчик, ни интегратор не возьмут на себя ответственность устанавливать ПО, отсутствующее в списке рекомендаций, потому что разработчик АСУ ТП может прекратить действие своей гарантии. В то же время в крупных организациях часто существуют свои корпоративные требования и стандарты, в связи с чем для разрешения данных противоречий и описанных проблем заказчик вынужден обращаться к специализированным организациям, имеющим опыт работы с различными производителями оборудования и программного обеспечения.

Преимущества комплексной защиты АСУ ТП компанией ЭЛВИС-ПЛЮС

Компания ЭЛВИС-ПЛЮС обладает большим опытом реализации систем защиты информации в различных отраслях и подходит к решению вопроса создания СЗ АСУ ТП комплексно и максимально независимо. Наша компания мультивендорная – это означает, что мы не привязаны к какому-то конкретному решению и ориентируемся на те условия, предпочтения и ограничения, которые есть у конкретного заказчика. При этом мы оказываем консультационные услуги и располагаем широким портфелем решений основных отечественных и иностранных производителей. При выборе продуктов мы больше ориентируемся на профессионализм вендора, на уровень его сервисной поддержки, на документированность, оперативность реагирования на запросы и то, насколько полно и комплексно продукт закрывает проблемы заказчика, а также на динамичность и перспективы развития самого продукта.

Основные преимущества комплексной системы защиты технологических систем и объектов:

- Данная система позволяет в первую очередь решать вопросы бизнеса. Информационную безопасность мы рассматриваем лишь как инструментарий, позволяющий решать проблемы заказчика.
- Комплексная система защиты, кроме того, предоставляет дополнительный механизм контроля и обеспечивает повышение прозрачности, контролируемости и эффективности работы организаций и промышленных предприятий.
- Система позволяет заказчикам реализовать потребность в соответствии нормативным требованиям, в том числе обязательным, за невыполнение которых следуют санкции и штрафы, а также административные и уголовные наказания.
- Комплексный подход нашей компании дает возможность решать проблему безопасности без ущерба основному бизнес-процессу заказчика, без остановки производства, отрыва сотрудников от рабочего процесса, с минимизацией влияния на производственные процессы организаций и промышленных предприятий. ●

NM
АДРЕСА И ТЕЛЕФОНЫ АО "ЭЛВИС-ПЛЮС" см. стр. 80