Пять причин

провести аудит информационной безопасности АСУ ТП в этом году

Алексей КОМАРОВ,
региональный представитель УЦСБ в Москве

Проблема обеспечения информационной безопасности (ИБ) автоматизированных систем управления технологическими процессами (АСУ ТП) активно (по крайней мере активнее, чем ранее) обсуждается уже несколько лет, однако по количеству реализуемых в указанной области проектов все еще преобладают аудиты и обследования. Примеров построения систем защиты информации не в пример меньше, и причины этого ясны: аудит АСУ ТП является первой ступенькой на пути к созданию комплексной системы защиты информации АСУ ТП. Вместе с тем, не для всех владельцев промышленных систем автоматизации очевидна необходимость того, что в этом направлении вообще нужно что-либо предпринимать. Рассмотрим основные причины, которые могут стать побудительными для проведения аудита информационной безопасности АСУ ТП.

Компоненты АСУ ТП содержат уязвимости

В основе промышленных систем автоматизации лежат программное обеспечение и аппаратные платформы, которые долгие годы разрабатывались с учетом требований, специфичных для указанной области применения: минимальные задержки, длительный бесперебойный режим работы и т. п. Вопросы информационной безопасности при этом оставались вне зоны внимания разработчиков – преобладали требования по обеспечению промышленной и функциональной безопасности.

Как отмечают эксперты, нередко защищенность современных веб-браузеров в разы лучше, чем программного обеспечения АСУ ТП: многие разработчики промышленных решений не используют даже методы защиты от переполнения буферов, встроенные в компиляторы и существенно усложняющие атаки на АСУ ТП. О более сложных методах защиты речь идет еще реже. На рис. 1 приведены обобщенные результаты исследования программного обеспечения низкоуровневых (полевых) устройств таких компаний, как ABB, Endress+Hauser, Emerson, Schneider Electric, Vega, Honeywell и др., показывающие положение вещей пусть в ограниченной области, но достаточно наглядно.

Не всегда уязвимости в программном обеспечении могут быть реализованы на практике, т. е. не для всех уязвимостей существуют коды – так называемые эксплойты, которые можно использовать для совершения вредоносных действий. Специализированные организации, такие как, например, ICS-CERT, регулярно публикуют обнаруженные исследователями уязвимости с описанием их влияния, перечнем конкретных продуктов, подверженных данной

Рис. 1. *Уязвимость программного обеспечения 752 различных устройств, поддерживающих низкоуровневый протокол Hart*

Источник: Digital Security

Рис. 2. *Количество обнаруженных уязвимостей в АСУ ТП*

Источник: Positive Technologies

уязвимости, и подробными рекомендациями по устранению потенциального негативного влияния.

На рис. 2 приведена статистика по количеству таких обнаруженных уязвимостей в АСУ ТП за период с 1997 по 2014 г. Стоит отметить, что всплеск после 2009 г. обусловлен скорее интересом к теме со стороны исследователей и увеличением числа проделанных работ по поиску уязвимостей, нежели реальным снижением степени защищенности.

В ходе аудита как раз и можно выявить наличие уязвимых компонентов в АСУ ТП. Компании, регулярно проводящие такие аудиты, могут выявить большее число уязвимостей, чем можно найти в открытых источниках, поскольку, например, некоторые найденные ранее уязвимости могут быть еще не опубликованы, так как вендор пока не выпустил соответствующее обновление либо такие уязвимости могут быть обнаружены непосредственно в ходе аудита. Количество разработчиков компонентов АСУ ТП велико, и для узкоспециализированных решений или кастомизированных продуктов широкие исследования могли еще просто не проводиться.

В АСУ ТП происходят инциденты ИБ

Инциденты информационной безопасности в АСУ ТП, к счастью, носят единичный характер (см. некоторые примеры инцидентов в табл. 1), и по каждому из них, даже самому широко известному и исследованному, все равно остаются вопросы и недосказанности. Пожалуй, только ситуация со знаменитым компьютерным червем Stuxnet не оставляет сомнений в том, что причина была именно во вредоносном ПО и что негативные последствия (выход оборудования из строя) действительно имели место.

В других же случаях может возникнуть ощущение, что причиной инцидента стали человеческий фактор или, например, неисправность оборудования, которую владельцы АСУ ТП пытаются скрыть за действиями злоумышленников и кибератаками. Причины недостаточности информации кроются в изначальной закрытости подобных систем, а также в банальном отсутствии средств анализа и мониторинга состояния информационной безопасности.

С другой стороны, если посмотреть, например, на интерактивную

Таблица 1. Некоторые инциденты ИБ АСУ ТП

Дата	Страна	Инцидент
Декабрь 2014	Германия	Федеральное управление по информационной безопасности признало факт компьютерной атаки на сталелитейный завод, в результате которой предприятию был нанесен ущерб
Февраль 2015	США	Хакеры атаковали автозаправочную станцию, скомпрометировав подключенную к Интернету систему управления насосными механизмами, контролирующими работу топливного хранилища
Март 2015	Россия	Специалисты уральских оборонных предприятий обнаружили необъяснимый сбой в иностранном оборудовании
Июнь 2015	Польша	Более десятка рейсов крупнейшей польской авиакомпании LOT отменены из-за хакерской атаки на ИТ-систему аэропорта Варшавы

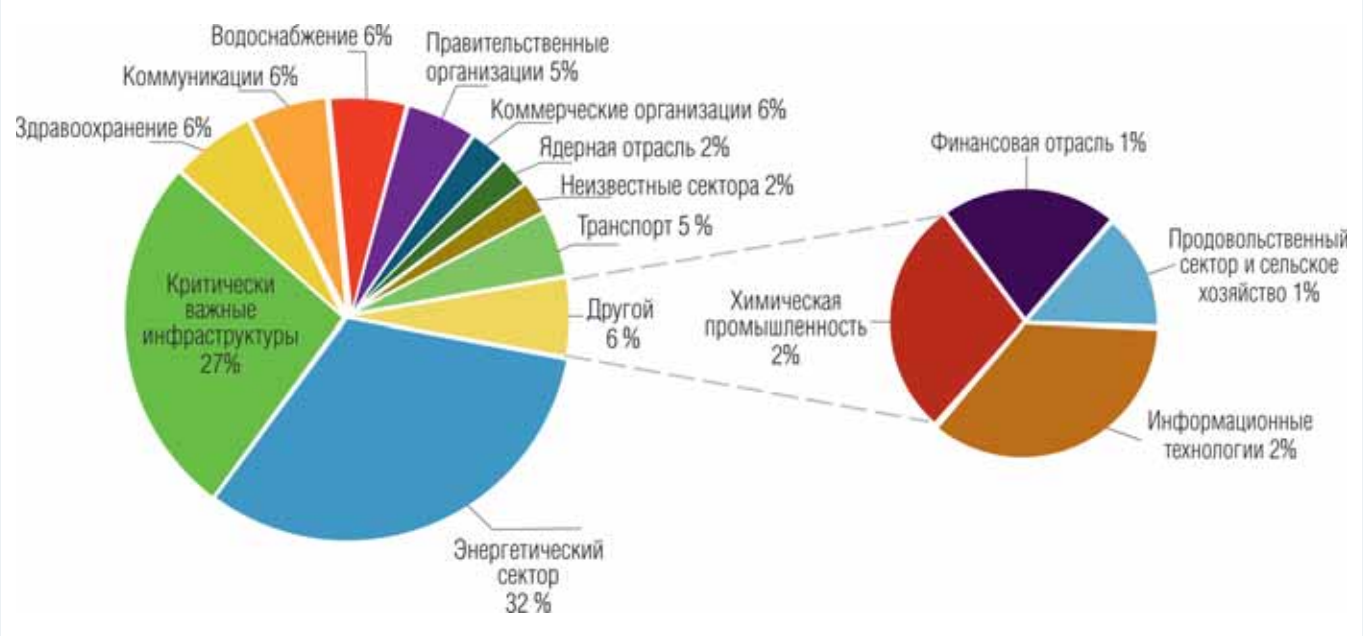

Рис. 3. *Распределение инцидентов по секторам промышленности в 2014 г.* *Источник: ICS-CERT*

карту Министерства энергетики Российской Федерации (http://www.minenergo.gov.ru/activity/management/info.php) с оперативной информацией по всем регионам России, то можно увидеть, что предусмотрены только следующие типы инцидентов: технологическое нарушение, чрезвычайная ситуация, стихийное бедствие, теракт. Отдельной категории для инцидентов информационной безопасности не предусмотрено, при этом на практике большая часть всех нештатных ситуаций помечается как чрезвычайная ситуация, а в кратких справках-докладах лишь фиксируется факт инцидента без детализации вызвавших их причин: *«В 00.40 действием защиты отключилась тупиковая ВЛ 110 кВ»*.

В российском законодательстве нет обязательного для всех владельцев промышленных систем требования публикации информации об инцидентах информационной безопасности, а глубокий анализ произошедших событий после факта восстановления работоспособности проводится редко, поэтому репрезентативную статистику по России собрать невозможно, но общую оценку ситуации можно получить на основании зарубежных источников. На рис. 3 приведена статистика инцидентов по секторам промышленности за 2014 г. от американской организации ICS-CERT по 245 зафиксированным инцидентам.

Недостаток информации о реальных инцидентах затрудняет расчет вероятности инцидентов, но, как правило, для критических инфраструктур даже единичное событие влечет тяжкие негативные последствия, поэтому может оказаться, что при любой ненулевой вероятности события цена, которую придется «заплатить», окажется слишком высокой – человеческие судьбы и жизни. К тому же отсутствие публичной информации не означает отсутствия в России инцидентов, в кулуарах конференций и выставок про инциденты рассказывают. Как показывает практика, порой одного показательного случая бывает достаточно для изменения отношения к самой проблеме информационной безопасности АСУ ТП в целой отрасли.

Оценка текущего уровня защищенности АСУ ТП

В конкурсной документации тендеров на проведение аудита ИБ АСУ ТП в качестве целей провер-

> Недостаток информации о реальных инцидентах затрудняет расчет вероятности инцидентов.

ки чаще всего используется именно такая (иногда с вариациями) формулировка: «оценка текущего уровня защищенности АСУ ТП».

Действительно, знания о наличии уязвимых компонентов АСУ ТП и ненулевой вероятности инцидентов не дают сами по себе понимания того, каков текущий уровень защищенности конкретной АСУ ТП.

В ходе анализа результатов аудитов предприятий металлургической

отрасли и ТЭК (более 30 производственных объектов и свыше 150 действующих АСУ ТП), проведенных специалистами компании УЦСБ (Уральский центр систем безопасности), было выявлено, что из принимаемых мер технической защиты только в 88% используются решения по сетевой безопасности, при этом для 17% АСУ ТП так или иначе организован удаленный доступ – из корпоративной сети, а иногда и через Интернет (табл. 2). Встроенные в АСУ ТП механизмы защиты применяются ограниченно, при том что антивирусные решения и большая часть программного обеспечения практически не обновляются.

Помимо технических мер на защищенность влияют меры организационные и физической безопасности. Возвращаясь к результатам упомянутого исследования компании УЦСБ, можно отметить, что у всех обследованных предприятий присутствует организационно-распорядительная документация, но лишь у 15% есть специалисты по информационной безопасности на производственных объектах, а эффективный контроль выполнения требований ИБ сторонними подрядчиками осуществляется слабо или вовсе не проводится.

Комплекс мер по физической безопасности в силу наличия требований законодательства и понятных рисков (например, хищения продукции) реализуется почти всегда, однако это зачастую не влияет на общий уровень защищенности информации вследствие концентрации на объектах, непосредственно связанных с производством, но не с управлением.

Результаты проводимых аудитов показывают актуальность защищенности АСУ ТП, но не всегда в качестве первоочередных мер требуются именно технические: повысить уровень защищенности можно и без приобретения дорогостоящих средств защиты. Определить правильные компенсирующие меры как раз и позволяет аудит информационной безопасности АСУ ТП, поскольку в его рамках можно показать вероятные сценарии реализации угроз ИБ.

Помимо технических мер на защищенность влияют меры организационные и физической безопасности.

Требования законодательства

Рассматривая аудит информационной безопасности в целом, а не только для АСУ ТП, нужно признать, что законодательные и/или отраслевые требования являются самым сильным мотивационным фактором, влияющим на принятие решения о проведении аудита. Скажем, в банковской сфере перед руководством не нужно обосновывать необходимость проведения аудита на соответствие требованиям стандартов PCI DSS, такой аудит проводится, причем ежегодно.

Законодательство в области информационной безопасности АСУ ТП пока носит скорее рекомендательный характер. Некое явное предписание, но общего характера можно встретить разве что в Федеральном законе Российской Федерации от 21.07.2011 № 256-ФЗ «О безопасности объектов топливно-энергетического комплекса», ст. 11 которого гласит:

«В целях обеспечения безопасности объектов топливно-энергетического комплекса субъекты топливно-энергетического комплекса создают на этих объектах системы защиты информации и информационно-телекоммуникационных сетей от неправомерного доступа, уничтожения, модифицирования, блокирования информации и иных неправомерных действий и обеспечивают функционирование таких систем».

При этом вопросы информационной безопасности промышленных объектов так или иначе затрагиваются в гораздо более широком спектре документов. В табл. 3 приведена информация об основной нормативной базе по вопросам обеспечения ИБ АСУ ТП на момент подготовки статьи. Несмотря на обилие документов, даже самый подробный из них – приказ ФСТЭК России № 31 – не является обязательным к исполнению, хотя он прошел регистрацию в Министерстве юстиции, о чем нередко говорят на публичных мероприятиях представители ФСТЭК России.

Тем не менее проекты по проведению аудита на соответствие

Таблица 2. Результаты аудита предприятий металлургической отрасли и ТЭК

Сетевая безопасность	• Обеспечивается для 88% объектов • Для 17% АСУ ТП есть удаленный доступ из корпоративной сети
Встроенные механизмы защиты	• HMI-аутентификация, режим киоска, ограничения доступа к меню • Системное ПО – по умолчанию • ПЛК – отключены
Антивирусная защита	• Применяется в 25% АСУ ТП • Обновляется в 11% АСУ ТП
Обновления	• Своевременные – для 8% АСУ ТП

Источник: Компания УЦСБ

Таблица 3. Нормативная база по обеспечению ИБ АСУ ТП	
Год	Документ
2007	Федеральный закон от 9.02.2007 № 16-ФЗ «О транспортной безопасности»
	Руководящий документ «Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры» (КСИИ) (утв. ФСТЭК России 18.05.2007)
	Руководящий документ «Общие требования по обеспечению безопасности информации в КСИИ» (утв. ФСТЭК России 18.05.2007)
	Руководящий документ «Методика определения актуальных угроз безопасности информации в КСИИ» (утв. ФСТЭК России 18.05.2007)
	Руководящий документ «Рекомендации по обеспечению безопасности информации в КСИИ» (утв. ФСТЭК России 19.11.2007)
2011	Федеральный закон Российской Федерации от 21.07.2011 № 256-ФЗ «О безопасности объектов топливно-энергетического комплекса»
2012	«Основные направления государственной политики в области обеспечения безопасности АСУ производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации» (утв. Президентом РФ 03.02.2012, № 803)
2013	Указ Президента Российской Федерации № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» от 15.01.2013
2014	Приказ ФСТЭК России № 31 от 14.03.2014 «Об утверждении требований к обеспечению защиты информации в АСУ производственными объектами и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей среды»
2016 (планы)	Документ ФСТЭК России «Меры защиты информации в АСУ»
	Документ ФСТЭК России «Методика определения угроз безопасности информации в АСУ»
	Документ ФСТЭК России «Порядок выявления и устранения уязвимостей в АСУ»
	Документ ФСТЭК России «Порядок реагирования на инциденты, связанные с нарушение безопасности информации»
	Федеральный закон «О безопасности КСИИ Российской Федерации» (законопроект ФСБ России)

требованиям приказа № 31 ФСТЭК России уже встречаются. С одной стороны, здесь срабатывает желание подготовиться заранее, до принятия соответствующего федерального закона, с другой – каких-либо других столь же конкретных требований не так много.

Что же такое АСУ ТП?

Одна из самых распространенных причин для проведения аудита ИБ АСУ ТП – желание подразделений информационной безопасности понять, что же на самом деле представляют собой автоматизированные системы управления технологическими процессами.

Не редкость и четкое разграничение сфер ответственности как на крупных территориально распределенных, так и на небольших локальных предприятиях: сотрудники, отвечающие за информационную безопасность, попросту не имеют доступа к промышленным сегментам и соответственно перед ними не ставятся задачи по обеспечению их безопасности. Даже в случае наличия сетевой связанности с корпоративным сегментом зона ответственности, как правило, ограничивается установкой межсетевого экрана на границе и настройкой VPN-соединения.

За сами технологические объекты и их бесперебойное функционирование отвечают другие – эксплуатирующие – подразделения, которые акцентируют внимание на непрерывности технологических процессов и, как отмечалось выше, сохранности продукции, а не на информационной безопасности и защите информации. В подобных ситуациях перед подразделениями информационной безопасности ставятся задачи по выработке той или иной позиции по вопросам ИБ АСУ ТП с целью понять, имеет ли смысл защищать АСУ ТП и тратить на это финансовые и человеческие ресурсы. Первым шагом для выработки такой позиции становится естественное желание понять состав АСУ ТП, ее функциональную структуру, возможные угрозы и потенциальный ущерб. Лучшим решением для детального изучения становится проведение аудита.

Заключение

Проведение аудита информационной безопасности АСУ ТП своими силами теоретически возможно, но на практике встречается редко и обычно предваряет внешний аудит, проводимый системным интегратором или специализированной консалтинговой компанией. Компаний, заявляющих о готовности провести коммерческий аудит защищенности АСУ ТП, достаточно много, поэтому критериями выбора конкретного исполнителя могут быть: наличие в штате квалифицированных специалистов, опыт аналогичных работ, сертификаты ФСТЭК России, ФСБ России и др., а также опыт реализации проектов по построению комплексных систем защиты АСУ ТП, поскольку аудит является лишь начальным этапом, а конечной целью должно быть повышение уровня защищенности АСУ ТП и в результате предприятия в целом.

Некоторые исполнители предлагают услугу тестового аудита, выполняя упрощенное обследование заранее оговоренной АСУ ТП, технологического процесса и/или объекта в течение нескольких рабочих дней с предоставлением краткого оптимизированного по содержанию итогового отчета. Такие пробные аудиты позволяют на практике, а не по рекламным материалам оценить возможности компании, качество работ и квалификацию специалистов до принятия решения о выборе исполнителя на комплексный проект по проведению аудита. ■