Оценка защищенности критически важных объектов

В последнее время вопросам обеспечения информационной безопасности АСУ ТП уделяется все больше внимания. Судите сами: на каждой выставке или конференции по ИБ есть специализированная секция, тематические выступления собирают полные залы слушателей, традиционные и интернет-издания если и не имеют специальных рубрик, то время от времени выпускают номера, главной темой которых становится ИБ АСУ ТП.
Вместе с тем в России разработаны (или готовятся) нормативные документы только верхнего уровня. Таким образом, мы уже знаем, КУДА двигаться. Но по-прежнему немало вопросов по регулирующим документам нижнего уровня, т. е. пока не определено, КАК достигать поставленных целей. В сложившейся ситуации мы можем полагаться только на собственный практический опыт и собственные методики.

Руслан СТЕФАНОВ,
руководитель направления защиты АСУ ТП, ОАО «ЭЛВИС-ПЛЮС»

Любой проект по обеспечению ИБ АСУ ТП должен начинаться с оценки защищенности. Компанией ЭЛВИС-ПЛЮС была разработана собственная методика оценки для предприятий электроэнергетики, которая базируется на нормативных документах ФСТЭК России, международных стандартах, большом опыте проведения аудитов ИБ на промышленных предприятиях и на зарубежных best practices. Следует отметить, что безусловным мировым лидером как по проработанности нормативной базы, так и по практическому применению разработок является отрасль электроэнергетики США. Там же проводится и большинство научно-исследовательских работ в этой сфере.

Практика показывает, что проблемы могут начаться еще на первом этапе процесса оценки защищенности – при формировании рабочей группы и подготовке аудита. Ведь в рабочую группу должны входить не только представители ИБ-службы и аудиторы, но и специалисты по эксплуатации и промышленной безопасности, поскольку при чрезвычайной ситуации на критически важном объекте (КВО) может быть причинен ущерб людям (сотрудникам КВО, жителям окрестностей) и окружающей среде. Но это привносит и свои трудности, поскольку задачи различных подразделений зачастую конфликтуют друг с другом: аудиторы должны найти уязвимости в информационных системах, служба эксплуатации – обеспечить непрерывность работы, «промбезопасники» – гарантировать безопасность всего процесса. Специалисты компании ЭЛВИС-ПЛЮС смогли найти решение и в этой ситуации. Передовой опыт подразумевает использование стендов и макетов, разворачивание в виртуальной среде образов АРМ и серверов, задействованных в техпроцессе, моделирование технологических систем и симуляция техпроцессов в опытных лабораториях. Это позволяет нам, не прекращая техпроцесс и без риска возникновения инцидентов на КВО, провести все необходимые пен-тесты и инструментальные проверки.

Одна из важнейших целей проведения аудита ИБ – определение целевого уровня безопасности объекта защиты или того, каким требованиям должен отвечать конкретный КВО. В рамках разработанной ЭЛВИС-ПЛЮС методики рассматриваются два типа уровней безопасности – целевой и достигнутый. Целевой определяет уровень защищенности конкретной системы, которому она должна соответствовать, исходя из оценки рисков. Достигнутый характеризует текущий уровень защищенности конкретной системы. Стандарт IEC 62443-1-1 предлагает пять уровней ИБ: нулевой – требования информационной безопасности отсутствуют; первый – защита от случайных или непреднамеренных нарушений (угроз); второй – защита от преднамеренных нарушений (угроз) с применением простых средств и минимальных ресурсов, требующих общих навыков и минимальной мотивации; третий – защита от преднамеренных нарушений (угроз) с использованием сложных средств и умеренных ресурсов, требующих специфичных для объекта защиты навыков и умеренной мотивации; четвертый – защита от преднамеренных нарушений (угроз) с применением сложных средств и максимальных ресурсов, требующих специфичных для объекта защиты навыков и максимальной мотивации.

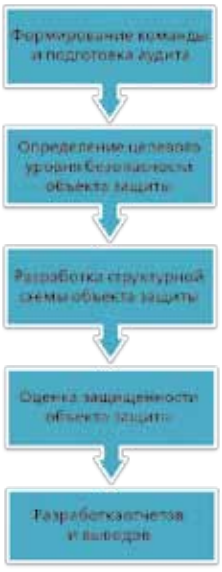
Для каждой технологической системы и/или зоны, в которой расположена система, должен быть установлен целевой уровень безопасности – направление будущего

движения в пространстве и метрики обеспечения ИБ. Его определяют с помощью моделирования угроз и оценки рисков, которое является вспомогательным методом для оценки рисков. Для оценки защищенности есть подходы и методики, основанные на различных метриках. Например, можно использовать метрики базы уязвимостей CVE (Common Vulnerabilities and Exposures компании MITRE). В CSET, созданном по заказу DHS США, применяется подсчет различных ответов на вопросы разных категорий с заданными весовыми коэффициентами. Выявление угроз осуществляется с помощью опросных листов, в которых вопросы делятся на три большие группы: вопросы, направленные на выявление источников угроз; вопросы, направленные на выявление уязвимостей; вопросы, направленные на выявление влияющих на управление технологическим процессом деструктивных действий. Далее все полученные угрозы классифицируются по величине возможного ущерба и вероятности реализации угрозы. Так мы можем оценить уровень риска с помощью всем понятных слов – от «низкого» до «недопустимого».

Каждому уровню риска и величине возможного ущерба соответствует свой целевой уровень безопасности. Если уровень риска выявленных актуальных угроз – «недопустимый», то целевым уровнем безопасности (УБ) будет максимальный, четвертый уровень. Целевой УБ нужно определять и по величине возможного ущерба. Для электроэнергетики специфичными показателями будут количество отключенных потребителей, длительность отключений, стабильность электропитания, потеря генерирующих мощностей. Конечно, это не исчерпывающий список, и он может быть расширен экспертами рабочей группы. Например, инцидент ИБ может вызвать отключение энергоснабжения на несколько недель, тогда целевой уровень ИБ КВО – третий, т. е. мы должны защитить нашу информационную систему «от преднамеренных нарушений (угроз) с применением сложных средств и умеренных ресурсов».

Следующим этапом является определение текущего уровня ИБ КВО. Для этого мы проводим оценку состояния ИБ с помощью опросных листов и инструментальных проверок по 25 параметрам, среди которых подсистемы ИБ, организационные меры, физическая безопасность объекта. На основании этих данных определяется, насколько текущее состояние ИБ КВО соответствует целевому уровню безопасности для конкретного объекта.

Такое обследование позволяет однозначно указать на те области, которые требуют первоочередного внимания для защиты объекта. По опыту наиболее уязвимыми местами технологических систем являются рабочие места операторов технологических процессов, требуют защиты сети передачи данных, службы управления учетными записями и контроля доступа. Очень часто не предприняты необходимые для обеспечения информационной безопасности организационные меры. На все это и должен указать аудитор заказчику.



Однако само по себе перечисление слабых мест в системе обеспечения безопасности информации не имеет большой ценности. Важны рекомендации по повышению уровня ИБ и разработка требований к системам защиты. Мы уже разрабатывали политики ИБ и требования к отдельным подсистемам обеспечения ИБ для нескольких компаний энергетического сектора России, где они успешно применяются.

В настоящий момент наша компания готова внедрять решения ведущих мировых и отечественных производителей, которые уделяют большое внимание ИБ КВО. В части защиты от вредоносного кода и контроля приложений – это Kaspersky Lab, Symantec и McAfee; межсетевые экраны – mGuard от Phoenix Contact, решения от Tofino Security; сканеры уязвимостей – Nessus от Tennable и российский MaxPatrol от Positive Technologies; управление доступом пользователей – Indeed-Id, контроль пользователей – ObserveIt. Основное требование к ним – установка и работа без прерывания технологического процесса.

Компания ЭЛВИС-ПЛЮС, как и вся отрасль в целом, уже готова защищать критически важные объекты. Теперь важно, чтобы операторы КВО поняли, что они не могут не реагировать на современные вызовы и угрозы. ■

Компания ЭЛВИС-ПЛЮС, как и вся отрасль в целом, уже готова защищать критически важные объекты. Теперь важно, чтобы операторы КВО поняли, что они не могут не реагировать на современные вызовы и угрозы.