ИБ в ключевых системах информационной инфраструктуры.
От теории к практике

Андрей КОНДРАТЕНКО,
Ведущий эксперт по ИБ,
ОАО «СО ЕЭС»

ОАО «СО ЕЭС» выполняет функции оперативного диспетчерского управления и АСУ ТП как таковых не имеет, однако участвует в управлении критически важными объектами. В статье представлены результат анализа требований ФСТЭК России, накопленный опыт и рекомендации по обеспечению информационной безопасности ключевых систем информационной инфраструктуры (КСИИ), который будет полезен организациям, приступающим к защите АСУ ТП.

Введение

Процесс обеспечения информационной безопасности АСУ ТП исторически воспринимался технологами как стремление «влезть» в их сферу деятельности и нарушить работу АСУ ТП. Попытки обосновать эту деятельности пресекались вопросом: «Покажите где это написано?» – и зачастую на этом останавливались.

Вместе с тем вопросы информационной безопасности и безопасности в целом становились актуальными после инцидентов, приводивших к катастрофам и человеческим жертвам. Вероятно, обратить особое внимание на вопросы ИБ заставят последствия какой-либо масштабной кибератаки на АСУ ТП.

Так или иначе, вышел Федеральный закон № 256-ФЗ от 21.07.2011 «О безопасности объектов топливно-энергетического комплекса», направленный в основном на антитеррористическую защищенность, но содержащий ст. 11, в которой затронуты вопросы информационной безопасности:

«1. 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...»

К сожалению, подзаконных актов, регламентирующих, как нужно защищать АСУ ТП объектов ТЭК, пока нет, однако федерального закона оказалось достаточно, чтобы проводить плановые работы по повышению ИБ АСУ ТП.

Еще до выхода закона регуляторами были разработаны документы, руководствуясь которыми можно повысить информационную безопасность АСУ ТП в целом. Детальный анализ документа, утвержденного Советом Безопасности Российской Федерации в 2005 г., «Система признаков критически важных объектов и критериев отнесения функционирующих в их составе информационно-телекоммуникационных систем к числу защищаемых от деструктивных информационных воздействий» и пакета документов ФСТЭК России по обеспечению ИБ в КСИИ, утвержденных в 2007 г., позволил сделать вывод, что среди систем, относящихся к КСИИ, упоминаются системы, работающие в отрасли электроэнергетики, и это в первую очередь АСУ ТП.

Таким образом, требования ФСТЭК России по обеспечению ИБ КСИИ применимы для повышения ИБ АСУ ТП.

Мероприятия по защите КСИИ

Мероприятия по защите КСИИ начинаются с ответов на вопросы: является ли объект КСИИ, к какому уровню важности КСИИ он относится и в соответствии с какими документами необходимо его защищать? При отнесении объекта к КСИИ рекомендуется утвердить документ (например, акт классификации), который станет основой как для планирования мероприятий по защите КСИИ, так и для контролирующих органов при проведении проверок.

Последовательность мероприятий по защите КСИИ такова:

- обследование текущего состояния информационной безопасности;
- моделирование угроз;

- разработка специальных технических требований (СТТ) по обеспечению безопасности информации;
- разработка и реализация проекта защиты;
- оценка соответствия защиты требованиям для КСИИ.

При реализации мероприятий разумнее пользоваться услугами внешних специализированных организаций, обладающих необходимыми лицензиями и компетенциями. Рекомендуется обеспечивать конфиденциальность документов, разрабатываемых в ходе проекта.

Обследование текущего состояния ИБ

Необходимо определить объекты обследования (например, объекты обследования на предмет отнесения к КСИИ могут располагаться не во всех зданиях организации или не во всех филиалах) и согласовать состав и формат результирующего отчета. Рекомендуется указать, по какой методике проводится обследование и на соответствие чему проводится проверка. Отчет должен содержать анализ структуры КСИИ и примерное описание технологического процесса, а также анализ текущих мероприятий по защите информации в КСИИ. В отчете должны быть выводы о правильности классификации КСИИ, основные выявленные несоответствия и предложения по последующим мероприятиям.

Результирующий отчет должен быть согласован с проверяемыми подразделениями. Какой бы уважаемой ни была внешняя организация, в отчете могут присутствовать расхождения предоставленной и интерпретированной информации, например, к КСИИ могут быть отнесены информационные системы, которые таковыми не являются, или могут быть сделаны ошибочные выводы о функциональности АСУ ТП.

Моделирование угроз

Моделирование угроз рекомендуется выполнять в соответствии с документами «Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры», «Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры» (утв. ФСТЭК России 18.05.2007).

Стоит учесть, что в АСУ ТП, относящихся к КСИИ, информация передается в режиме реального времени и основные требования к ней – доступность и целостность, в то время как требований по конфиденциальности может не быть вовсе.

Модель угроз должна содержать анализ наличия вероятных нарушителей безопасности информации в АСУ ТП, рисков, актуальных угроз безопасности информации и возможных последствий реализации угроз. Результатом моделирования являются также выводы об отнесении АСУ ТП к КСИИ одного из сегментов информационной и телекоммуникационной инфраструктуры России и уровне ее важности.

Разработка СТТ

Для организации защиты АСУ ТП как КСИИ рекомендуется разработать специальные технические требования (СТТ). Требования должны быть актуальны именно для данного уровня важности (класса) КСИИ. При их составлении должны быть учтены результаты обследования текущего состояния ИБ и моделирования угроз.

Формирование СТТ рекомендуется выполнять в соответствии с документами «Общие требования по обеспечению безопасности информации в ключевых системах информационной инфраструктуры» (утв. ФСТЭК России 18.05.2007), «Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры» (утв. ФСТЭК России 19.11.2007). Разработанные СТТ целесообразно направить на экспертизу в профильное подразделение ФСТЭК. С одной стороны, это позволит проверить, насколько правильно были восприняты и применены требования ФСТЭК, с другой – при проведении проверок контролирующими органами согласованные СТТ будут доказательством того, что защита АСУ ТП строится в соответствии с требованиями ФСТЭК России к КСИИ.

Проект защиты

Проект защиты АСУ ТП должен отражать перечень организационных и технических мер, которые должны быть реализованы для выполнения СТТ по ИБ. Утвержденный проект должен стать основой для построения системы информационной безопасности АСУ ТП и инвестиционного планирования обеспечения безопасности КСИИ.

Оценка соответствия

Для оценки соответствия реализованной защиты планируемому уровню ИБ целесообразно проводить аттестацию АСУ ТП как объекта информатизации. Аттестацию имеет право проводить организация, имеющая лицензию ФСТЭК. Срок полной реализации мероприятий по защите АСУ ТП как КСИИ может составить два-три года.

Требования по защите информации

Требования по защите информации в КСИИ можно разделить на несколько направлений:

- защита от несанкционированного доступа:
  - управление доступом;
  - регистрация и учет;
  - обеспечение целостности;
- антивирусная защита;
- безопасность межсетевого взаимодействия;
- обнаружение вторжений;
- анализ защищенности;
- контроль отсутствия НДВ.

Сформированные СТТ помогут понять, какие требования по ИБ уже выполняются в организации, какие системы внедрены и могут быть использованы для выполнения требований по КСИИ, какие системы нужно модернизировать, какие – внедрять заново.

Стоит обратить внимание, что для обеспечения (повышения) доступности АСУ ТП необходимо применять принципы дублирования (например, каналов связи) и «горячего» резервирования (сетевого оборудования, серверов).

Защита от несанкционированного доступа

Задачи защиты от несанкционированного доступа (НСД) могут

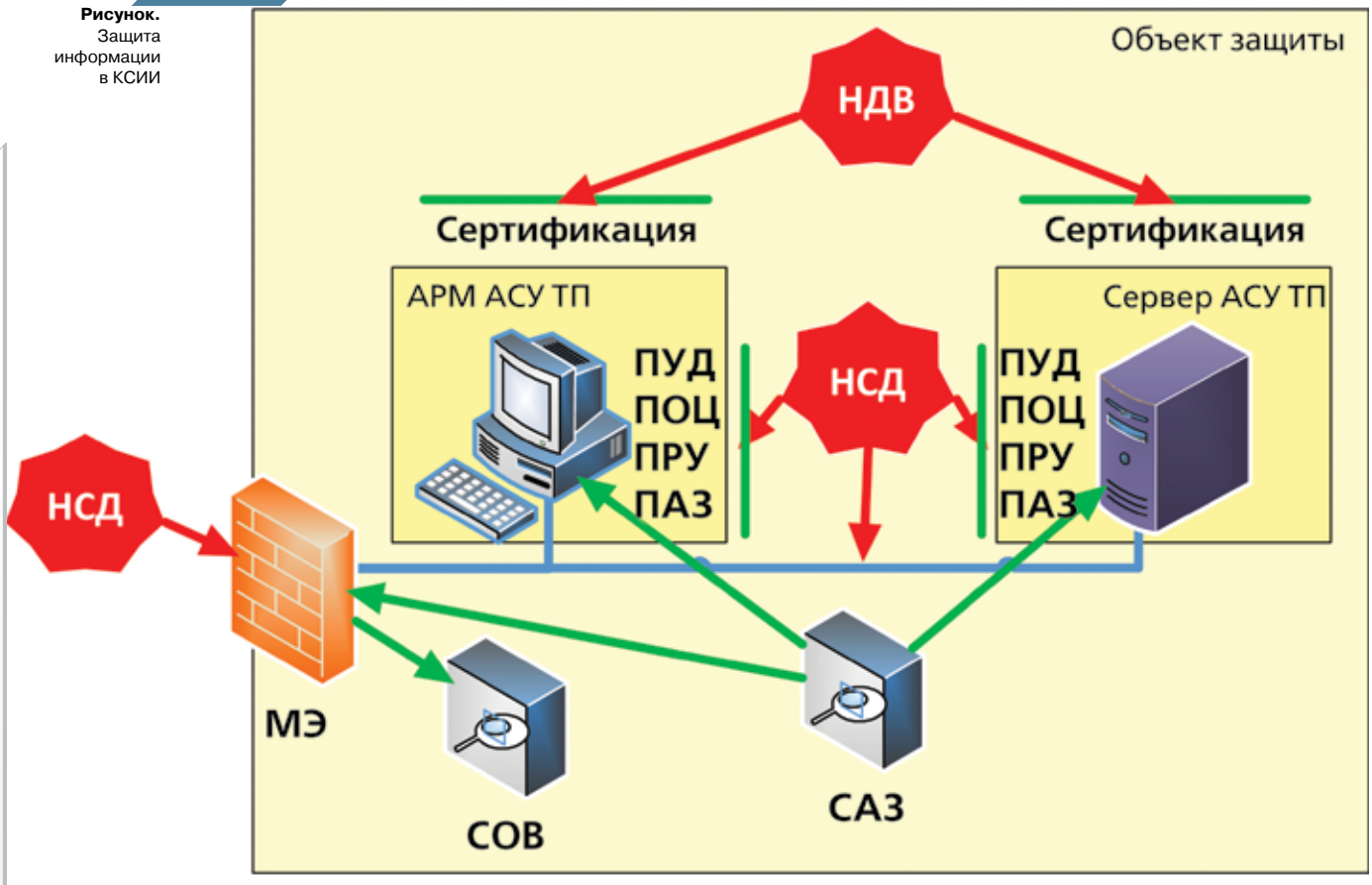

Рисунок. Защита информации в КСИИ

решаться отдельными подсистемами или уже быть учтенными в других системах.

Подсистема управления доступом (ПУД) должна осуществлять идентификацию, проверку подлинности и контроль доступа субъектов в систему, к устройствам, программам, файлам и т. п. в зависимости от класса защищаемой АСУ ТП. Для проверки используются механизмы аутентификации с использованием паролей, сертификатов, биометрии, карт доступа и др. Чем сложнее и важнее информационная система, тем строже требования по управлению доступом.

Подсистема регистрации и учета (ПРУ) должна осуществлять контроль входа/выхода субъектов в/из защищаемой автоматизированной системы. В зависимости от сложности поставленных задач подсистема может вести журналы событий – от входа и выхода пользователей в систему в самых простых случаях до подробной записи любых действий всех субъектов взаимодействия с информацией (добавления, удаления, изменения, просмотр, печать и т. д.).

Подсистема обеспечения целостности (ПОЦ) должна обеспечивать целостность программных средств защиты информации, самой обрабатываемой информации, а также неизменность программной среды. Целостность обычно проверяется при загрузке операционной или информационной системы путем сравнения контрольных сумм (CRC) программ и информации в самых простых случаях. К более серьезным системам разрабатываются требования по оперативному контролю и воздействию на безопасность АС, периодическому тестированию функций защиты с помощью специальных программных средств, наличию автоматических средств восстановления при сбоях. Это особенно актуально для систем, где сложно обеспечить физическую защиту от вмешательства и оперативный выезд специалиста.

Перечисленные подсистемы – ПУД, ПРУ, ПОЦ – в зависимости от требований по информационной безопасности к информационным системам могут быть реализованы:

- средствами операционной системы (ОС);
- специализированными средствами защиты информации;
- встроенными средствами АСУ ТП путем приведения ее в соответствие требованиям руководящих документов.

У каждого метода реализации есть свои подводные камни.

При защите от НСД средствами сертифицированной ОС параметры ОС необходимо настроить в соответствии с требованиями/рекомендациями руководящих документов, но требования к настройке могут быть таковы, что КСИИ не будет работать. Кроме того, ОС нужно периодически обновлять, а сертификат на ОС после обновления будет недействительным.

При обеспечении защиты от НСД наложенными средствами могут возникнуть проблемы обеспечения работоспособности КСИИ в режиме реального времени, так как присутствующие на рынке наложенные средства,

адаптированные для защиты государственной тайны и конфиденциальной информации, не учитывают особенности работы систем реального времени.

При обеспечении защиты от НСД средствами АСУ ТП необходимо проводить доработку ПО и сертификацию. На текущий момент требования к сертифицированным средствам защиты избыточны для ПО АСУ ТП и поэтому трудно реализуемы (например, есть требования по очистке памяти, хотя конфиденциальной информации в АСУ ТП как КСИИ может не быть; по применению дискреционного и мандатного доступа, а не ролевого; запрещение использования идентификации/аутентификации средствами ОС). Вместе с тем современное ПО для АСУ ТП может использовать методы аутентификации и авторизации смежных систем (например, аутентификации с использованием Active Directory, хранения правил авторизации в СУБД SQL), при этом смежные системы могут быть не сертифицированными, а их сертификация экономически нецелесообразной. Для встроенных в АСУ ТП средств защиты от НСД следует проводить сертификацию в специализированной аттестованной лаборатории и по решению ФСТЭК России.

Для выбора метода защиты от НСД необходимо учитывать много факторов и в первую очередь требования конкретной КСИИ по доступности.

Антивирусная защита

Для организации, имеющей доступ в сеть Интернет, рекомендуется создание эшелонированной антивирусной защиты, где оборонительными эшелонами являются:

- почтовые и интернет-шлюзы, проверяющие входящий интернет-трафик (в том числе на наличие спама);
- антивирус на почтовом сервере;
- антивирус на файловых серверах, серверах приложений и баз данных;
- антивирус на рабочих станциях и АРМ.

Непосредственно в КСИИ используются антивирусы на файловых серверах и на АРМ, подключенных к КСИИ.

При использовании антивирусов в КСИИ существуют риски:
а) блокирования технологического ПО;
б) замедления работы технологического ПО.

Блокирование технологического ПО может произойти, если сигнатура антивируса сработает на каком-то из исполняемых файлов технологического ПО. Чтобы такого не происходило, целесообразно исключить из антивирусной проверки исполняемые модули либо отправить исполняемые модули в антивирусную компанию, чтобы сделать их «доверенными» для антивируса.

Замедление работы технологического ПО происходит в моменты массовых антивирусных проверок исполняемых файлов и папок на АРМ и серверах. Поэтому приходится переносить проверки системы на время технологических окон в работе КСИИ, исключать из проверки папки баз данных реального времени.

Следует помнить, что антивирусные решения требуют постоянного обновления сигнатур, и на это нужно планировать бюджет.

Безопасность межсетевого взаимодействия

Безопасность межсетевого взаимодействия обеспечивается межсетевыми экранами (МЭ). Межсетевой экран должен быть настроен в соответствии с правилами межсетевого экранирования, принятого в организации, и в соответствии с правилами, необходимыми и достаточными для работы сегмента КСИИ. Рекомендуется, используя МЭ, отделять технологический сегмент сети и КСИИ от локальной вычислительной сети организации.

Межсетевые экраны должны быть сертифицированы по классу защищенности в органах сертификации ФСТЭК России. Сертификат на МЭ выдается на три года, после чего необходимо его продление либо сертификация новой версии прошивки МЭ. Это необходимо учесть при планировании финансирования. При наличии несертифицированного МЭ и невозможности замены его сертифицированным можно провести его сертификацию с привлечением сертификационной лаборатории.

Прошивки МЭ могут периодически обновляться, обновления могут быть платными. В случае обновления МЭ сертификат будет считаться недействительным. Поэтому необходимо взвесить, какая угроза является более актуальной – нарушение функционирования КСИИ или несоответствие сертификата требованиям регулятора.

На рынке существуют недорогие МЭ с небольшой пропускной способностью и дорогие стабильно работающие промышленные МЭ. Для КСИИ рекомендуется выбирать вторые и покупать их комплектом для настройки «горячего» резервирования.

Обнаружение вторжений

Компоненты систем обнаружения вторжений (СОВ) более известны как IPS (Intrusion Prevention System) и IDS (Intrusion Detection System). Технически один и тот же компонент может выполнять обе роли – предотвращения и обнаружения: тогда в первом случае он ставится вразрез принимаемого трафика, а во втором работает с зеркальной копией трафика. Однако при установке компонентов в режиме IPS может резко снизиться доступность распределенной информационной системы. Это происходит, если изменения в системе происходят часто и не контролируются теми, кто настраивает фильтры сигнатур, а также в случае выхода новых сигнатур обнаружения вторжений.

Обычно СОВ подключается в режиме IDS к SPAN-порту пограничного устройства сети (для защиты от внешних угроз) или пограничного устройства сегмента КСИИ (для защиты от внутренних угроз). После первичного включения СОВ необходимо проводить тюнинг каждого его компонента – настройку сигнатур детектирования в соответствии с правилами работы сети.

Квалифицированный технический персонал должен осуществлять мониторинг срабатывания сигнатур и проводить разборы инцидентов ИБ. Сигнатурное поведение СОВ необходимо подстраивать при изменении правил

работы сети и защищаемых сегментов. СОВ может показать весь аномальный трафик не только по настроенным правилам работы сети, но и по сигнатурам, ежедневно обновляемым ведущими компаниями-производителями.

Для соответствия регуляторным требованиям компоненты СОВ для КСИИ настраиваются в соответствии с профилями защиты ФСТЭК России.

Как и для антивирусов, для СОВ необходимо постоянно обновлять базу сигнатур. Сертифицированная СОВ и ежегодная покупка лицензии на обновление сигнатур обойдутся довольно дорого.

Анализ защищенности

Система анализа защищенности (САЗ) выполняет контроль настроек защиты операционных систем на рабочих станциях и серверах, безопасности программного обеспечения. С ее помощью производятся сканирование сети в целях исследования ее топологии, поиск незащищенных или несанкционированных сетевых подключений, проверки настроек межсетевых экранов и т. п. Средства сканирования уязвимостей могут функционировать на сетевом уровне, уровне операционной системы и уровне приложения. С помощью сканирующего ПО можно составить карту доступных узлов информационной системы, выявить используемые на каждом из них сервисы и протоколы, определить их основные настройки и сделать предположения относительно вероятности несанкционированного доступа. По результатам сканирования системы вырабатываются рекомендации и меры по устранению выявленных недостатков.

В САЗ присутствуют два режима анализа: audit и pentest.

Для режима audit необходимы учетные записи исследуемого оборудования с правами администратора. Режим audit гарантирует, что не будет выполнено никаких деструктивных действий на проверяемом оборудовании. Результатом проверки является отчет обо всех расхождениях в текущих настройках и версиях операционных систем с рекомендациями производителей и аналитиков.

В режиме pentest САЗ ведет себя как хакер, подбирая учетные данные и «ломая» системы с использованием известных уязвимостей. Не следует запускать режим pentest на действующей КСИИ даже во время технологического окна. Для него рекомендуется использовать полигон КСИИ.

Некоторые САЗ предоставляют режим compliance – расширение, позволяющее проводить аудит на соответствие собственным установленным политикам, а также сравнивать результаты прежних аудитов.

Таким образом, при включении САЗ рекомендуется:

- проводить для КСИИ аудит не в автоматическом периодическом режиме, а по заявке, с информированием эксплуатирующих служб;
- тщательно выбирать оборудование для аудита и проводить аудит порциями (например, по одной заявке сетевое оборудование, по другой – серверное, по третьей – АРМ). Это позволит сократить размер технологического окна и сконцентрироваться на конкретных задачах.

В зависимости от функциональности ПО САЗ требует разной квалификации персонала. Анализ с использованием свободно распространяемых утилит может выполнить только опытный инженер. Сертифицированное ПО стоит дорого, но с ним может справиться пользователь, обладающий средней компетенцией в вопросах ИБ. При покупке ПО необходимо планировать деньги на ежегодное обновление сигнатур.

Контроль отсутствия НДВ

Для ПО, используемого при защите информации в КСИИ (в том числе когда функции защиты информации встроены в прикладное ПО КСИИ), должен обеспечиваться определенный уровень контроля недекларированных возможностей. Контроль отсутствия НДВ осуществляется путем сертификации ФСТЭК России. Проведение сертификации требует затрат по доработке ПО, оформлению разработчиком документации в соответствии с требованиями ФСТЭК, оплате услуг сертификационной лаборатории. Но эти затраты приемлемые.

Есть несколько вариантов сертификации ПО. Сертификацию экземпляра целесообразно проводить, когда требуется ПО для одного объекта; сертификацию партии – когда нужно одно ПО для нескольких объектов; сертификацию производства – когда ПО постоянно находится в стадии доработки и расширения.

Выводы

Требования по защите АСУ ТП не всегда выполнимы (поэтому их нужно тщательно адаптировать для своей организации), но достаточны для того, чтобы повысить информационную безопасность АСУ ТП.

Требования регуляторов не учитывают особенностей АСУ ТП в части обеспечения доступности, текущих (тесной интеграции с ОС) и новых (виртуализация) реалий.

В организации должны быть специалисты по ИБ, досконально разбирающиеся в вопросах ИБ АСУ ТП и работе АСУ. Специалисты внешней организации их заменить не смогут, а способны только дополнить.

Наложенные сертифицированные средства защиты от НСД (неправильная настройка или ложное срабатывание) могут нарушить доступность АСУ.

Выполнять требования регуляторов по ИБ для готовой системы АСУ ТП достаточно дорого, поэтому необходимо учитывать требования ИБ на стадии замысла и создания АСУ ТП, это позволит существенно снизить затраты на ИБ при внедрении системы.

При обеспечении ИБ возникают проблемы, выходящие за рамки компетенции специалистов по ИБ: отсутствует законодательный акт, обязывающей выполнять требования по защите КСИИ, – пока это только рекомендации регулятора; стоимость средств для обеспечения защиты систем очень высока и сопоставима со стоимостью самой системы, иногда и выше. ■