МИТРЕЙКИН
Александр Николаевич -
кандидат экономических наук,
советник заместителя министра
энергетики Российской Федерации
Адрес: 107996, ГСП-6, г. Москва,
ул. Щепкина, 42
e-mail: mitreykin_an@mail.ru

Некоторые аспекты обеспечения безопасности АСУ ТП в ТЭК России

Автоматизированная система управления технологическим процессом (АСУ ТП) - комплекс программных и технических средств, предназначенный для автоматизации управления технологическим оборудованием на предприятиях.

Как правило, АСУ ТП характеризуются тем, что обеспечивают комплексную автоматизацию технологических операций на всем производстве или отдельном участке, выпускающем относительно завершенный продукт.

Комплекс АСУ ТП включает в себя распределенную систему управления (РСУ) и системы противоаварийной автоматической защиты (ПЗА). РСУ, в свою очередь, представляет собой программно-аппаратный комплекс, состоящий из Контрольно-измерительных приборов и автоматики (КИПиА), Программируемого логического контроллера (ПЛК) и Человеко-машинного интерфейса (станция оператора, станция инженера, станция инженера КИПиА).

Связь между элементами АСУ ТП осуществляется через промышленную цифровую сеть, по которой с централизованного пульта управления или с отдельных устройств для обеспечения диспетчеризации команды поступают к исполнительным устройствам или контроллерам. Обратную связь обеспечивают при помощи разнообразных датчиков.

Составными частями АСУ ТП могут быть отдельные системы автоматического управления (САУ) и автоматизированные устройства, связанные в единый комплекс. Обычно АСУ ТП имеет единую систему операторского управления технологическим процессом в виде одного или нескольких пультов управления, средства обработки и архивирования информации о ходе процесса, типовые элементы автоматики: датчики, контроллеры, исполнительные устройства.

Независимые исследования показывают, что практически в любой автоматизированной системе управления производством (АСУП), АСУ ТП можно обнаружить множественные уязвимости, которые способны привести к нарушению корректной работы технологического процесса и реализации угроз несанкционированного доступа к информации, обрабатываемой в:

- системах диспетчерского управления и сбора данных (SCADA);
- отдельных интерфейсах управления объектами автоматизации;
- элементах телеметрической подсистемы и телемеханики;
- прикладных приложениях для анализа производственных и технологических данных;
- системах управления производством (MES-системы).

Исходя из мирового опыта, можно обозначить следующие наиболее часто встречающиеся уязвимости:

- исполнение произвольного кода (неавторизированное, авторизированным пользователем);
- загрузка и исполнение произвольных файлов;
- отказ в обслуживании;
- уязвимости, вызывающие повышение привилегий;
- раскрытие информации для доступа к базе данных.

Реализация некоторых из перечисленных уязвимостей позволяет остановить технологический процесс, что может негативно отразиться на ходе его отдельных потоков и привести к аварийной ситуации.

Многие популярные системы диспетчеризации (SCADA - Supervisory Control And Data Acquisition, Диспетчерское управление и сбор данных) базируются на платформе операционной системы Microsoft Windows, в связи с чем отдельной угрозой, частично использующей штатные методы для исполнения, является распространение вредоносного кода для кражи критически важных данных о проектах технологических процессов и нарушения их корректной работы. Поэтому необходимо обеспечивать информационную безопасность используемой для программно-аппаратного комплекса АСУП и АСУ ТП операционной системы, на которую устанавливается прикладное программное обеспечение.

В качестве примера, обосновывающего серьезность последней упомянутой угрозы, можно привести появление компьютерного червя Stuxnet - первого широко известного компьютерного червя, перехватывающего и модифицирующего информационный поток между программируемыми логическими контроллерами марки и рабочими станциями одной широко распространенной SCADA-системы. Таким образом, червь может быть использован в качестве средства несанкционированного сбора данных (шпионажа) и диверсий в АСУ ТП промышленных предприятий, электростанций, аэропортов и т.п.

Упомянутый компьютерный червь обладает рядом характеристик, позволяющих оценить его как первый пример серьезной угрозы АСУ ТП:

- целенаправленно ищет и заражает компьютеры с установленной АСУ ТП определенного производителя;

- модифицирует программы в контроллерах, которые через частотно-регулируемые приводы определенных моделей и конкретной конфигурации управляют скоростью вращения электродвигателей;
- проводит атаку посредством перевода управляемого оборудования в нештатный режим (для диспетчеров на компьютерах воспроизводится запись нормального режима работы, а возможность диспетчера безопасно остановить оборудование блокируется);
- использует четыре неизвестные ранее уязвимости MS Windows для распространения;
- способен распространяться через сменные носители, по локальной сети, через интернет и по промышленной шине Profibus;
- собирает и передает информацию о зараженных компьютерах (версия ОС, сетевой адрес и т.п.), а также обновляется через интернет;
- применяет специальные приемы уклонения от антивирусов;
- скрывает свое присутствие на зараженном компьютере.

Необходимо отметить, что понятие о безопасности в сетях и информационных системах предприятий и компаний значительно отличается от понятия безопасности для АСУ ТП и АСУП. Если для первых наиболее важна конфиденциальность данных, то для систем управления технологическими процессами и производством на первом месте находится безопасность персонала, оборудования, самих технологических процессов. Отсюда следуют и различия в подходах к обеспечению безопасности рассматриваемых автоматизированных информационных систем, к используемым при этом инструментам. При этом необходимо учитывать, что угрозы безопасности АСУ ТП могут возникать как извне, так и изнутри защищаемой сети / системы.

В качестве некоторых основных угроз в области информационной безопасности в энергетике можно выделить следующие:

- уже упомянутое активное создание вредоносного программного обеспечения, коммерциализация этого процесса, приводящая к созданию вредоносных программных комплексов, снабженных различными инструментами взлома систем защиты информации, а также технической поддержкой (например, поддержкой по обновлению вредоносного кода);
- использование спама (массовой рекламной рассылки без согласия получателя) и фишинга (кражи или получения обманным путем конфиденциальных данных с целью их дальнейшего использования для получения денежных средств, рассылки спама и т.д.);
- утечки информации, связанные как с проникновением злоумышленников извне, так и со сбором и передачей инсайдерской (внутренней) информации;
- проблемы, связанные с квалификацией работников компаний в области информационной безопасности;
- несогласованность действий сторон в процессе передачи и использования информации, в том числе составляющей коммерческую тайну.

Перечень перечисленных проблем далеко не полон, однако хотелось бы остановиться на ключевой из обозначенных угроз - проблеме квалификации работников организации, особенно тех, в задачи которых входит обеспечение информационной безопасности, в том числе безопасности АСУ ТП. На предприятиях и в компаниях при проведении системной работы по обеспечению безопасности автоматизированных информационных систем необходимо вводить и соблюдать особые требования к такому персоналу.

Указанные работники, занимающиеся анализом текущего состояния существующих систем обеспечения информационной безопасности в ТЭК, внутренней и внешней нормативной правовой базы, регулирующей обеспечение информационной безопасности, должны обладать следующими навыками и знаниями:

- состава и перспектив развития критически важных объектов управления производством и технологическими процессами, командных (управляющих) и измерительных систем, используемых в организации, в том числе тех, нарушение штатного режима функционирования которых может привести к значительному вреду для производственных процессов и повлечь за собой негативные последствия для Российской Федерации;
- архитектуры, состава, принципов и особенностей работы информационно-управляющих (в том числе используемых для управления непрерывными технологическими процессами), командных, измерительных и информационно-телекоммуникационных систем, предназначенных для управления критически важными объектами организации и/или для информационного обеспечения управления такими объектами;
- методов и способов обеспечения безопасности, в том числе информационной безопасности, применяемых на критически важных объектах управления производством и технологическими процессами организации;
- регламентации деятельности субъектов в области обеспечения безопасности информации в информационно-телекоммуникационных системах для недопущения реализации возможных угроз безопасности информации или минимизации ущерба от их реализации и сохранения устойчивого и безопасного функционирования объектов ТЭК России.

Работники, обеспечивающие безопасность АСУ ТП и АСУП, должны выбираться из числа работников подразделений (служб), обеспечивающих развитие и внедрение информационных технологий и эксплуатацию телекоммуникационных сетей, информационную безопасность, а также отвечающих за устойчивое функционирование технологических процессов обеспечения деятельности критически важных объектов ТЭК.

Необходимо отметить, что промышленно развитые страны, такие как Соединенные Штаты Америки, достаточно серьезно относятся к проблеме защищенности АСУ ТП и АСУП своих промышленных объектов не только от террористических, но и от кибератак (метод информационной войны осуществляется путем воздействия на узлы в информационной сети с целью прекращения их работы или их деструктивного изменения). Подтверждением этому могут стать следующие факты:

- США оставляют за собой право на использование всех необходимых средств, включая военную силу, в случае проведения против них крупной кибератаки (доклад «Международная стратегия по киберпространству»);
- работа по подготовке и принятию закона об информационной безопасности (CyberAct);
- проведение исследований и разработок Министерством обороны США в области информационной безопасности («кибербезопасности»);
- периодическое проведение масштабных учений по противостоянию информационной угрозе CyberStrorm;
- 12 инициатив Президента США Барака Обамы по кибербезопасности государства и т.д.

Так, в мае 2011 г. из открытых источников стало известно, что американские компании, в управлении ко-

торых находятся объекты критически важной инфраструктуры (в том числе и объекты топливно-энергетического комплекса), должны будут сотрудничать с правительственными органами, чтобы обе стороны были убеждены в надежности критически важных инфраструктур. При этом Департамент национальной безопасности США получает право требовать от этих компаний выполнения тех или иных дополнительных норм по промышленной безопасности. Указанная инициатива властей США получила неофициальное название CyberAct.

В России работа по обеспечению информационной безопасности критически важных объектов ведется Советом Безопасности Российской Федерации, профильными федеральными органами исполнительной власти, такими как ФСБ России, ФСТЭК России, а также отраслевыми федеральными органами исполнительной власти.

В частности, в Минэнерго России в конце 2010 г. приказом министра создана соответствующая рабочая группа, целями деятельности которой являются:

- проведение анализа текущего состояния существующих систем обеспечения информационной безопасности в ТЭК;
- анализ существующей нормативной правовой базы, регулирующей обеспечение информационной безопасности в области ТЭК.

Результатом деятельности рабочей группы должно стать заключение о состоянии дел в сфере обеспечения информационной безопасности автоматизированных систем управления производством и технологическими процессами объектов ТЭК России, а также план мероприятий по совершенствованию мер, направленных на обеспечение информационной безопасности упомянутых объектов.

В свете стремительно растущих темпов проникновения информационных технологий в нашу жизнь, широкого использования автоматизированных систем управления производством и технологическими процессами, не являющимися полностью изолированными от открытых систем, следовательно, от различного рода угроз информационной безопасности, а также с учетом соответствующих инициатив таких государств, как Соединенные Штаты Америки, Китайская Народная Республика, работа по обеспечению безопасности критически важных объектов топливно-энергетического комплекса Российской Федерации в части защиты от информационных угроз должна быть активизирована компаниями ТЭК во взаимодействии с соответствующими федеральными органами исполнительной власти.

Литература:

1. ESET: новый червь Win32/Stuxnet атакует промышленные компании. [Электронный ресурс]. - Режим доступа: http://www.esetnod32.ru/.company/press/index.php?id=7952#

2. Американские власти рассекретили инициативы по кибербезопасности. [Электронный ресурс]. - Режим доступа: http://www.securitylab.ru/news/391320.php

3. Обзор инцидентов информационной безопасности АСУ ТП зарубежных государств. [Электронный ресурс]. - Режим доступа: http://www.securitylab.ru/analytics/398184.php

4. Приказ Минэнерго России от 11.11.2010 № 541-дсп «О рабочей группе по обеспечению информационной безопасности объектов топливно-энергетического комплекса».

5. Т.А. Пьявченко, В.И. Финаев. Автоматизированные информационно-управляющие системы. - Таганрог: Изд. ТРТУ, 2007. - 271 с.

НАША ИНФОРМАЦИЯ

Бюллетень № 5 Российского энергетического агентства «Анализ выполнения положений Федерального закона № 261»

Вышел в свет 5-й номер Бюллетеня, издаваемого Российским энергетическим агентством Минэнерго России «Анализ выполнения положений Федерального закона № 261 от 23.11.2009 г. "Об энергосбережении и повышении энергетической эффективности, внесении изменений в отдельные законодательные акты Российской Федерации» в бюджетной сфере в разрезе федеральных округов и регионов Российской Федерации по состоянию на 01.04.2011 г.”». Бюллетень публикует результаты исследования активности субъектов Российской Федерации в выполнении данного закона.

Впервые в Российской Федерации мониторинг энергосбережения в бюджетной сфере регионов и муниципальных образований в I квартале 2011 г. осуществлялся на основе использования созданного в ФГБУ «РЭА» Автоматизированного рабочего места «Мониторинг энергоэффективности. Регламентированная отчетность» (далее АРМ).

Разработка, ввод в опытную, а затем в промышленную эксплуатацию в апреле 2011 года единой автоматизированной информационной системы ввода, обработки данных по энергосбережению в бюджетной сфере, имеющей АРМ, распределенные по иерархическим уровням - здание; учреждение; орган местного самоуправления; администрация региона; Российская Федерация, - позволили значительно повысить прозрачность всего процесса сбора и ввода данных, а также достоверность, верифицируемость и скорость обработки информации.

Применение автоматизированной системы с большим количеством абонентов системы (более 140000 региональных и муниципальных учреждений), а также принятое решение использовать АРМ при сборе и обработке данных по итогам I квартала 2011 г., потребовали от ФГБУ «РЭА» проведения в короткий период большой работы по обучению, консультированию абонентов автоматизированной информационной системы в учреждениях, органах местного самоуправления, администрациях регионов, а также по техническому сопровождению и совершенствованию разработанной программы.

В настоящее время в большинстве региональных филиалов ФГБУ «РЭА» созданы учебно-консультационные пункты, проводятся информационные и методические семинары для ответственных лиц в учреждениях, муниципальных образованиях, региональных администрациях.

В Бюллетене №5 приводятся рейтинги активности регионов в выполнении ФЗ №261 в разрезе федеральных округов по состоянию на 1 апреля 2011 г., а также анализируется состояние разработки нормативно-правовой базы энергосбережения федеральными органами исполнительной власти и субъектами Российской Федерации на 1 апреля 2011 г., а также региональные программы энергосбережения.