А. А. Балаев, Т. А. Кондратьева

МЕТОДИКА АТТЕСТАЦИОННЫХ ИСПЫТАНИЙ PLC-СЕТЕЙ НА СООТВЕТСТВИЕ ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Ранее на основе тестирования локальной вычислительной plc-сети и сравнения результатов с технологией wi-fi [1] были показаны ее определенные достоинства и перспективы развития. Поэтому актуальна проблема обеспечения защиты информации в такой сети и, прежде всего, проверка эффективности применения традиционных методов и средств.

Целью данной статьи является описание методики проведения проверки plc-сети на соответствие требованиям безопасности информации. Данная методика основывается на положениях руководящих документов ФСТЭК России [2] и типовых методиках испытаний объектов информатизации по требованиям безопасности информации [3].

Проверка plc-сети на соответствие требованиям безопасности информации включает в себя выполнение следующих организационно-технических процедур контроля:

1. Защиты информации от несанкционированного доступа.
2. Целостности данных.
3. Эфективности криптографических средств защиты информации.

Защита информации от НСД

Целью испытаний является установление соответствия объектов информатизации требованиям РД Гостехкомиссии России «Автоматизированные системы. Защита от НСД к информации. Классификация АС и требования по защите информации» [4]. Испытания проводятся в следующем объеме [3]:

— проверка механизмов идентификации/аутентификации;
— проверка механизма контроля доступа;
— испытания подсистемы регистрации и учета;
— испытания подсистемы обеспечения целостности.

Испытания подсистемы управления доступом

Идентификация, проверка подлинности и контроль доступа субъектов, определенные требованиями по безопасности информации к установленному классу АС, должны осуществляться:

— при входе в систему по идентификатору (коду) и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов;

— при доступе к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ по логическим именам и/или адресам;

— при доступе к программам, томам, каталогам, файлам, записям, полям записи по именам.

Результаты испытания считаются удовлетворительными в случае выполнения следующих условий:

— все попытки взаимодействовать с объектами сети отклоняются, до тех пор пока не будет представлен криптографически стойкий идентификатор;

— средства управления требуют, чтобы каждый пользователь был успешно аутентифицирован до разрешения любого действия, выполняемого от имени этого пользователя;

— при вводе пароля, не соответствующего предъявленному идентификатору, средства управления обеспечивают задержку между попытками осуществить аутентификацию, достаточную, чтобы противодействовать возможности локального или удаленного перебора;

— при вводе пароля, не соответствующего предъявленному идентификатору, средства управления обеспечивают такую обратную связь, при которой попытки использования механизма аутентификации не будут приводить к превышению уровня вероятности подбора аутентификатора;

— при вводе пароля, не соответствующего предъявленному идентификатору, средства управления приостанавливают процесс предоставления доступа;

— при неоднократном вводе пароля, не соответствующего предъявленному идентификатору, средства управления прекращают процесс предоставления доступа;

— при вводе пароля, соответствующего предъявленному идентификатору, субъекту доступа должен быть предоставлен доступ в систему в соответствии с его полномочиями.

Для проверки механизма контроля доступа производятся:

— проверка соответствия реально установленных средств СЗИ НСД правилам разграничения доступа (ПРД), матрице разграничения доступа субъектов plc-сети к ее объектам;

— проверка непротиворечивости установленных ПРД;

— выборочные попытки реализовать НСД.

При установлении факта соответствия ПРД матрице доступа и блокировки произведенных попыток НСД реализация механизма доступа считается удовлетворенной.

Подсистема обеспечения целостности должна включать в себя:

— обеспечение целостности программных средств и обрабатываемой информации;

— физическую охрану средств вычислительной техники и носителей информации, а также каналов связи;

— наличие администратора (службы) защиты информации в plc-сети;

— периодическое тестирование СЗИ от НСД;

— наличие средств восстановления СЗИ НСД;

— использование сертифицированных средств защиты.

Надежность функций контроля целостности программных средств СЗИ НСД, обрабатываемой информации и программной среды проверяется при помощи внесения измерений в отдельные их компоненты или подмены этих компонентов. При этом фиксируется реакция системы защиты на произведенные нарушения.

Испытание функции контроля целостности считается успешным, если выполняются следующие условия:

— в автоматизированных системах отсутствуют средства разработки и отладки программ;

— перечень ресурсов, целостность которых подлежит контролю, соответствует требованиям руководящих документов для установленного класса защищенности plc-сети;

— при загрузке системы автоматически проверяется целостность контролируемых ресурсов по критериям, заданным руководящими документами для установленного класса защищенности plc-сети;

— при выявлении нарушений целостности контролируемых ресурсов должен выводиться отчет об этом, а обработка информации блокироваться для всех субъектов доступа, кроме пользователя с правами администратора;

— в случае если диаметр сети превышает 200 метров, используются ретрансляторы;

— основная и резервная кабельные линии электропитания должны быть проложены по разным трассам, исключающим возможность их одновременного выхода из строя.

Проверяется наличие и работоспособность технологии внесения новых программных средств в операционную среду, предусматривающую экспертную оценку или верификацию новых программных средств, для выполнения потенциально опасных для СЗИ программных функций. Оцениваются критерии санкционирования ввода программ в операционную среду и допуска определенных категорий пользователей к этим программам.

Проверяется наличие и работоспособность средств и мер предотвращения несанкционированного ввода программ в операционную среду.

Проверяется наличие и работоспособность процедур периодического тестирования всех функций СЗИ НСД, наличие графика проведения тестирования.

Проверяется наличие и работоспособность технологии восстановления программных средств защиты информации, ведение архива программных средств защиты.

Автоматическое оперативное восстановление функций СЗИ НСД при сбоях поверяется путем моделирования сбойных ситуаций и последующей проверки функций СЗИ НСД.

Производится проверка на устойчивость plc-сети к заражению вирусами или иными видами разрушающего программного воздействия. Испытания считаются успешными, если выполняются следующие условия:

— подтверждается наличие сертифицированного антивирусного программного обеспечения для обнаружения и сканирования компьютеров и носителей информации;

— проводятся регулярные инвентаризации программного обеспечения;

— подтверждается наличие процедуры проверки всех файлов на носителях информации сомнительного или неавторизованного происхождения или файлов, полученных из общедоступных сетей, на наличие вирусов перед работой с этими файлами;

— подтверждается наличие мероприятий, направленных на повышение компьютерной грамотности персонала;

— подтверждается наличие документированной политики, требующей соблюдения лицензионных соглашений и устанавливающей запрет на использование неавторизованного программного обеспечения;

— выполняется проверка на корректность работы антивирусного программного обеспечения. Для этой цели производится попытка внедрения в систему тестовой программы — вируса. Проверка считается успешной в случае обнаружения и блокирования попытки заражения штатными антивирусными средствами plc-сети.

Криптографические средства защиты информации

Результаты испытания считаются удовлетворительными в случае выполнения следующих дополнительных условий:

— определены методики использования криптографических средств в организации, включая общие принципы, в соответствии с которыми следует защищать информацию;

— определены принципы управления ключами, а также методы восстановления зашифрованной информации в случае потери, компрометации или повреждения ключей;

— установлены роли и обязанности должностных лиц, отвечающих за:

- реализацию политики,
- управление ключами.

Подготовка отчетной документации

Состоит в документальном оформлении протоколов испытаний и заключения по результатам испытаний с выводами о соответствии (или несоответствии) plc-сети требованиям по безопасности информации.

Результаты испытаний по всем рассмотренным выше направлениям обеспечения безопасности информации оформляются заключениями.

На основании полученных результатов испытаний оформляется общее заключение, которое включает:

— оценку соответствия plc-сети требованиям по безопасности информации;

— перечень выявленных недостатков и нарушений;

— рекомендации по устранению выявленных недостатков и нарушений.

В случае несоответствия plc-сети установленным требованиям и нормам защищенности информации необходимо оперативно устранить выявленные недостатки и нарушения.

При этом могут рекомендоваться следующие меры:

— исключение отдельных средств из состава plc-сети;

— проведение сертификационных испытаний отдельных средств plc-сети;

— применение дополнительных организационно-технических мероприятий по защите информации;

— доработка организационно-распорядительной документации;

— применение дополнительных сертифицированных средств защиты информации;

— исключение отдельных программных средств из состава plc-сети.

СПИСОК ЛИТЕРАТУРЫ:

1. *Балаев А. А., Горбатов В. С., Сепашвили Д. Т.* Тестирование безопасности PLC-технологии передачи данных // Безопасность информационных технологий. 2011. № 1. С. 57–60.

2. Федеральная служба технического и экспортного контроля. URL: http://www.fstec.ru.

3. Практическое руководство по основам правовой защиты информации, включая сборник правовых и технических документов. URL: http://www.lghost.ru/lib/security/kurs4/theme03_chapter02.htm#03.

4. Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации». URL: http://www.fstec.ru/_docs/doc_3_3_004.htm.