УДК 004.056

Ряба Е.И., Черниш Л.Г., Бабич А.Я.

ПРОГРАММНО-АППАРАТНЫЕ КОМПОНЕНТЫ КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

В статье рассмотрены основные принципы построения комплексных систем защиты информации. Проанализированы методы защиты информации, и приведен минимальный список рекомендованных средств защиты.

Ключевые слова: Комплексная система защиты информации, средства защиты информации, межсетевой экран, антивирус, криптографическая защита, аппаратные средства защиты.

Вступление. Комплексная система защиты информации (КСЗИ) представляет собой совокупность организационных и технических мероприятий, аппаратных и программных средств, обеспечивающих защиту информации в информационно-телекоммуникационных системах: на автономных рабочих станциях (АС класса 1) и в компьютерных сетях (АС класса 2 и 3). КСЗИ обеспечивает обработку информации, защита которой является обязательной и регулируется законом Украины «О защите информации в автоматизированных системах» и «О доступе к публичной информации». Система обеспечивает надежную защиту этой информации в процессах получения, использования, распространения и хранения.

Анализ последних исследований и постановка проблемы. Вопросы построения систем защиты информации рассмотрены в источниках, приведенных в конце статьи, однако в исследованиях не рассматривается список основных составляющих. *Актуальность* изысканий на тему построения систем защиты информации чрезвычайно высока в наш век компьютерных технологий. *Целью* текущей работы является описание основных составляющих программно-технического метода зашиты информации.

Основная часть. Комплексная система защиты информации включает мероприятия и средства, реализующие способы, методы, механизмы защиты информации от:

• утечки информации по техническим каналам (побочные электромагнитные излучения, акустоэлектрических каналы и т.д.);

• несанкционированных действий и несанкционированного доступа к информации (подключение к аппаратуре и линиям связи, маскировки под зарегистрированного пользователя, применение закладных устройств или программ и т.д.);

• специального воздействия на информацию (формирование полей и сигналов с целью нарушения целостности информации или разрушения системы защиты).

Программно-технический метод включает следующие средства:

• инженерно-технические средства реализуются в виде автономных устройств и систем и выполняют функции общей защиты объектов, на которых обрабатывается информация. К ним относятся, например, устройства защиты территорий и зданий, замки на дверях, где расположены аппаратура, решетки на окнах, электронно-механическое оборудование охранной сигнализации.

• под аппаратными техническими средствами принято понимать устройства, встраиваемые непосредственно в вычислительную технику, в телекоммуникационную аппаратуру, или устройства, работающие с подобной аппаратурой по стандартному интерфейсу. В настоящее время существует широкий спектр таких устройств

• программные средства составляет совокупность программного обеспечения, для идентификации пользователей, контроля доступа, шифрования информации, уничтожения временных файлов, тестового контроля системы защиты и прочее. Использование программных средств защиты информации имеет ряд преимуществ - универсальность, гибкость, надежность, простота в использовании то возможность модификации. [1,2,3]

Имея ввиду всё вышеописанное можно определить минимальный набор средств для защиты информации в автоматизированных системах:

Аппаратные средства. На рынке постоянно появляются новые средства промышленного шпионажа, в том числе, сверхминиатюрные средства съема информации и более чувствительные системы регистрации побочных излучений и наводок.

Произошел переход на цифровые методы кодирования, осваиваются ранее неиспользуемые частотные диапазоны, снижается энергопотребление, массогабаритные характеристики и, следовательно, повышается скрытность работы.

Одновременно развиваются устройства противодействия негласному получению информации.

Для получения новых тактических возможностей расширяется диапазон рабочих частот, повышаются чувствительность, разрешение, степень автоматизации обработки получаемых данных и уровень эргономичности конструктивных решений, обработанные результаты выводятся оператору в более простом и удобном виде, снижаются вес и габариты.

Существенное преимущество перед другими получают сканерных приемники, имеющие возможность работы под управлением компьютера или так называемые программно-аппаратные комплексы (ПАК). Использование внешней ПЭВМ с программным обеспечением позволяет автоматизировать процесс поиска и обнаружения закладных устройств.

Высокая степень автоматизации позволяет проводить анализ радиоэлектронной обстановки по районам контроля, вести базу радиоэлектронных средств и использовать ее для эффективного обнаружения радиозакладок. В том числе при кратковременных сеансах их работы, например, при использовании радиозакладок с дистанционным управлением, промежуточным накоплением информации (разделением этапов съема и передачи информации) и полуактивных закладных устройств.

Малый вес и габариты комплексов в сочетании с универсальным питанием (12 В, 220 В), встроенные батареи позволяют работать с ними в салоне автомобиля, в стационарных и полевых условиях. [4]

Криптографические методы. Готовое к передаче информационное сообщение, первоначально открытое и незащищенное, зашифровывается и тем самым превращается в шифрограмму, т.е. в закрытый текст или графическое изображение документа. В таком виде сообщение передается по каналу связи. Санкционированный пользователь после получения сообщения дешифрует его (т.е. раскрывает) посредством обратного преобразования криптограммы, вследствие чего получается исходный, открытый вид сообщения, доступный для восприятия санкционированным пользователям.

Методу преобразования в криптографической системе соответствует использование специального алгоритма. Действие такого алгоритма запускается уникальным числом (последовательностью бит), обычно называемым шифровальным ключом.

Для большинства систем схема генератора ключа может представлять собой набор инструкций и команд, либо компьютерную программу, или все это вместе, но в любом случае процесс шифрования (дешифрования) реализуется только этим специальным ключом. Чтобы обмен зашифрованными данными проходил успешно, как отправителю, так и получателю, необходимо знать правильную ключевую установку и хранить ее в тайне.

Устойчивость любой системы закрытой связи определяется степенью секретности используемого в ней ключа. Тем не менее, этот ключ должен быть известен другим пользователям сети, чтобы они могли свободно обмениваться зашифрованными сообщениями. В этом смысле криптографические системы также помогают решить проблему аутентификации (установления подлинности) принятой информации. Взломщик в случае перехвата сообщения будет иметь дело только с зашифрованным текстом, а истинный получатель, принимая сообщения, закрытые известным ему и отправителю ключом, будет надежно защищен от возможной дезинформации.

Современная криптография знает два типа криптографических алгоритмов: классические алгоритмы, основанные на использовании закрытых, секретных ключей, и новые алгоритмы с открытым ключом, в которых используются один открытый и один

закрытый ключ (эти алгоритмы называются также асимметричными). Кроме того, существует возможность шифрования информации и более простым способом - с использованием генератора псевдослучайных чисел.

Использование генератора псевдослучайных чисел заключается в генерации гаммы шифра с помощью генератора псевдослучайных чисел при определенном ключе и наложении полученной гаммы на открытые данные обратимым способом.

Антивирусная защита. Антивирусная защита состоит из:

• общие средства защиты информации. Сюда входит копирование информации (создание копий системных областей дисков и файлов), и разграничение доступа (предотвращение несанкционированного использования информации).

• профилактические меры, позволяющие уменьшить вероятность заражения вирусом;

• Специализированные программы для защиты от вирусов.

Общие средства защиты информации очень важны для защиты от вирусов, но все же их одних недостаточно. Должно иметь место применение специализированных программ для защиты от вирусов. Эти программы можно разделить на следующие виды:

Детекторы. Находят файлы, зараженные известными им вирусами.

Врачи. Очищают зараженные программы, удаляя из них тело вируса, тем самым восстанавливая программу в «здоровом» состоянии.

Ревизоры. Делают «снимки» состояния программ в их нормальном функционировании, а затем сравнивают при каждом новом запуске. При выявлении несоответствий сообщают пользователю.

Врачи-ревизоры. Сочетающие в себе свойства ревизоров и врачей. Такие программы, не только обнаруживают изменения в файлах и системных областях дисков, но и могут автоматически вернуть их в исходное состояние.

Фильтры. Постоянно находятся в оперативной памяти компьютера и перехватывают обращения к системе, которые, по их мнению, используются вирусами для воспроизведения и нанесения вреда, и сообщают о них пользователю.

Вакцины. Меняют программы и диски таким образом, что тот вирус, от которого производится вакцинация, считает их уже зараженными. На работу самих программ вакцинация не влияет. [5]

Межсетевые экраны. Фаервол, брандмауэр, сетевой экран - устройство или набор устройств, сконфигурированных чтобы допускать, отказывать, шифровать, пропускать через прокси весь компьютерный трафик между областями разной безопасности согласно набором правил и других критериев.

Фаервол может быть в виде отдельного прибора (так называемый маршрутизатор или роутер), или программного обеспечения, устанавливаемым на персональный компьютер или прокси-сервер.

В зависимости от соединений, отслеживаемых, файерволы разделяют на:

• stateless (простая фильтрация), которые не отслеживают текущие соединения (например TCP), а фильтруют поток данных исключительно на основе статических правил;

• stateful (фильтрация с учетом контекста), с отслеживанием текущих соединений и пропуском только пакетов, удовлетворяющих логике и алгоритмам работы соответствующих протоколов и программ. Такие типы файерволов позволяют эффективно бороться с различными DoS-атаками и уязвимостью некоторых протоколов сетей.

Для того чтобы удовлетворить требованиям широкого круга пользователей, существует три типа файерволов: сетевого уровня, прикладного уровня и уровня соединения. Каждый из этих трех типов использует свой, отличный от других подход к защите сети.

• Фаервол сетевого уровня представлен экранирующим маршрутизатором. Он контролирует только данные сетевого и транспортного уровней служебной информации пакетов. Минусом таких маршрутизаторов является то, что еще пять уровней остаются неконтролируемыми. Наконец, администраторы, работающие с экранирующими маршрутизаторами, должны помнить, что в большинстве приборов, осуществляющих фильтрацию пакетов, отсутствуют механизмы аудита и подачи сигнала тревоги. Иными

словами, маршрутизаторы могут подвергаться атакам и отражать большое их количество, а администраторы даже не будут проинформированы.

• Фаервол прикладного уровня также известен как прокси-сервер (сервер-посредник). Фаерволы прикладного уровня устанавливают определенное физическое разделение между локальной сетью и Internet, поэтому они соответствуют высоким требованиям безопасности. Однако, поскольку программа должна анализировать пакеты и принимать решения по контролю доступа к ним, файерволы прикладного уровня неизбежно уменьшают производительность сети, поэтому в качестве сервера-посредника используются более быстрые компьютеры.

• Фаервол уровня соединения похож на фаервол прикладного уровня тем, что оба они являются серверами-посредниками. Отличие состоит в том, что файерволы прикладного уровня требуют специального программного обеспечения для каждой сетевой службы вроде FTP или HTTP. Зато, файерволы уровня соединения обслуживают большое количество протоколов.

Выводы. Для каждой конкретной информационно-телекоммуникационной системы состав, структура и требования к КСЗИ определяются свойствами обрабатываемой информации, классом автоматизированной системы и условиями ее эксплуатации. В деле обеспечения информационной безопасности успех может принести только комплексный подход, который должен включать в себя минимальный рекомендуемый набор средств по защите информации, описанный в этой статье.

ЛИТЕРАТУРА

1. Степко О. М. Анализ основных составляющих информационной безопасности / О. М. Степко // Вісник НАУ. – 2009. – с. 83-92

2. Бойченко О. В. Особенности противодействия компьютерной преступности // О. В. Бойченко, М. М. Новіков // ФП.-2010-1. – с. 34-37.

3. Дудикевич В. Б. Концептуальные модели защиты информации // В. Б. Дудикевич, Ю. Р. Герасим, Г. В. Микитін // Львівська політехніка. – 2010. – с. 18-26.

4. Пархоменко И. И. Основные методы разведки в телекоммуникационных системах и методы противодействия // И. И. Пархоменко, А. Я. Бабич // Європейський університет. – 2011. – с. 131-133.

5. Бабич О. Я. Компьютерные вирусы и методы защиты от них // А. Я. Бабич, О. О. Мелешко, Д. Д. Рахманов // Vedecky prumysl evropskeho kontinentu. – 2010. – с. 67-71.

Надійшла: 15.12.2011

Рецензент: д.т.н., проф. Петров О.С.