УДК 004

М.В. Клокова, А.В. Чернышова
Донецкий национальный технический университет
Кафедра прикладной математики и информатики
E-mail: marizombie@outlook.com, alla@pmi.dgtu.donetsk.ua

АНАЛИЗ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В КОРПОРАТИВНЫХ СЕТЯХ

Аннотация

Клокова М.В., Чернышова А.В. Анализ средств защиты информации в корпоративных сетях. *В данной статье проведен анализ современных методов и способов защиты информации в корпоративных сетях. Рассмотрены криптографические средства, основные алгоритмы шифрования данных, технологии защиты от проникновений в сеть, а также составлен список требований к системам комплексной защиты информации для поддержания высокого уровня безопасности как внутри сети, так и при отправке данных за ее пределы.*

Актуальность

“Жить – значит быть источником и приемником информации” (А. Конопатский). Информация в современном обществе – одна из самых ценных вещей в жизни, требующая защиты от несанкционированного проникновения лиц, не имеющих к ней доступа. За последние несколько лет значительно возрос интерес частных и государственных компаний на рынке средств защиты информации.

Изложение материалов исследования

Для защиты информации применяются различные меры и способы, начиная с организационно-режимных и кончая применением сложных программно-аппаратных комплексов.

Одним из путей решения проблемы защиты информации, а точнее - решения небольшой части вопросов из всего спектра мер защиты, является криптографическое преобразование информации.

Криптографическими средствами защиты называются специальные средства и методы преобразования информации, в результате которых маскируется ее содержание. Основными видами криптографического закрытия являются шифрование и кодирование защищаемых данных. Рассмотрим подробнее саму суть шифрования.

Шифрование – обратимое преобразование информации в целях сокрытия от неавторизованных лиц, с предоставлением, в это же время, авторизованным пользователям доступа к ней. Этим занимается наука о методах обеспечения конфиденциальности – криптография. Задача криптографии, т.е. тайной передачи, возникает только для информации, которая нуждается в защите. В таких случаях считается, что информация содержит тайну или является защищаемой, приватной, конфиденциальной, секретной. [1]

Существует множество разных криптографических алгоритмов. Назначение этих алгоритмов — защита информации. Защищать же информацию приходится от разных угроз и разными способами. Чтобы обеспечить надежную и адекватную защиту с помощью криптоалгоритма (КА), нужно понимать, какие бывают КА и какой тип алгоритма лучше приспособлен для решения конкретной задачи.

Алгоритм симметричного шифрования требует наличия одного ключа для шифрования и дешифрования сообщений. Такой ключ называется общим секретным, поскольку все пользователи, участвующие в обмене данными, имеют один и тот же ключ.

Алгоритм асимметричного шифрования требует использовать один ключ для шифрования данных и другой, но взаимосвязанный с ним ключ — для дешифрования. Один из ключей в такой схеме доступен любому, кто его запрашивает.

Такой ключ называется открытым. Другой ключ известен только владельцу и называется секретным.

Внедрение криптосредств в системы защиты персональных данных

На сегодняшний день деятельность большинства крупных компаний связана с обработкой персональных данных различного типа, к защите которых выдвигается ряд требований. Прежде чем их выполнить, руководству компании необходимо построить модель угроз персональным данным и на ее основе разработать систему защиты, в состав которой должно входить средство криптографической защиты информации (СКЗИ).

Внедренное в систему защиты персональных данных СКЗИ должно соответствовать следующим требованиям:

- криптографическое средство должно штатно функционировать совместно с другими техническими и программными средствами;
- при обработке персональных данных для обеспечения их безопасности должны использоваться сертифицированные криптосредства.

По уровням защиты криптографические средства делят на 6 классов: КС1, КС2, КС3, КВ1, КВ2, КА1. Выбор определенного класса средств напрямую зависит от субъекта атаки (нарушителя), категория которого становится известна благодаря оператору в модели угроз. [2]

Средства криптографической защиты сегодня эффективно используются компаниями и организациями для защиты персональных данных и являются одной из важнейших составляющих в системах защиты персональных данных.

Защита корпоративной информации

Применительно к компаниям шифрование обычно используется в трех случаях, а именно в целях обеспечения безопасности хранения данных, защиты информации при

передаче через открытые каналы связи и по локальной сети и, наконец, для цифровых подписей. Все представленные задачи решаются разными средствами с применением различных криптографических технологий.

Итак, еще одно применение СКЗИ – это защита конфиденциальной информации компании. В сфере компьютерной безопасности для защиты корпоративной информации используется два принципиально разных подхода к защите от проникновений в сеть.

Первый и более старый из них это IDS (Intrusion Detection Systems). IDS – это система призванная обнаружить попытки проникновения в частную сеть и сообщить системному администратору о факте вторжения. Эта технология защиты информации используется довольно давно и уже завоевала популярность среди заказчиков.

Однако, многие аналитики считают, что сегодня существует более эффективный и удобный способ борьбы с хакерами. Эта система – Intrusion Prevention System, IPS, которая служит для предотвращения нападений. Под ней подразумевается набор технологий, которые появились на стыке межсетевых экранов и систем обнаружения нападений IDS. От межсетевых экранов в IPS взят принцип активного вмешательства в сетевое взаимодействие или поведение программ, а от IDS – интеллектуальные методы мониторинга происходящих событий. Таким образом, IPS не только обнаруживает нападения, но и пытается предотвратить их.

Среди продуктов IPS выделяют пять составляющих, каждая из которых может как работать самостоятельно, так и комбинироваться с другими. Это сетевая IDS, коммутаторы седьмого уровня, экран приложений, гибридные коммутаторы и ловушки.

Следует отметить, что IPS разных типов хорошо интегрируются в достаточно интеллектуальную систему защиты, в которой каждый элемент дополняет другие. При этом они не конкурируют с уже существующими средствами

информационной безопасности: межсетевыми экранами, IDS, антивирусами и др., поскольку дополняют их. [3]

Отдельное внимание стоит уделить технологии виртуальных защищенных сетей (Virtual Private Network). VPN способна обеспечить конфиденциальность, целостность данных и имитостойкость на уровне IP-пакетов. На основе этой технологии обеспечивается защищенное соединение между подсетями и компьютерами.

Технология VPN может работать с множественными алгоритмами шифрования и сложными конфигурациями тоннелей и защищенных периметров. Криптографическая стойкость обеспечивается применением соответствующих криптографических алгоритмов (3DES, AES, ГОСТ).

Главное преимущество данной технологии – прозрачность работы системы защиты: приложения работают так же свободно, как и в открытой сети, ничего не подозревая о работе VPN. [4]

Утечка информации

Согласно последним исследованиям, для многих IT компаний в последнее время стали проблемой инсайдеры – сотрудники, которые либо намеренно, либо случайно становятся источниками утечки информации. По мнению А. Крячкова, директора по продуктам компании Aladdin - ведущего разработчика и поставщика средств аутентификации, продуктов и решений для обеспечения информационной безопасности и защиты конфиденциальных данных в России – рекомендации по защите весьма просты. По его словам необходимо лишь следовать концепции 3A (Аутентификация, Авторизация, Аудит). Данная концепция основывается на следующих требованиях:

- доступ к критичным ресурсам компании должен быть персонифицированным, что позволяет снизить риск отказа пользователей от совершенных ими действий;
- необходимо применять шифрование критически важных данных, представляющих сферу особого интереса инсайдера;

- ключевая информация и другие секретные данные пользователя должны храниться на личном съемном носителе (например, на смарт-карте или USB-ключе), что повысит личную ответственность каждого сотрудника;
- в качестве профилактики и для снижения риска утечки информации важно проводить регулярный мониторинг всех действий пользователей в сети.

А.П. Кекишев, главный инженер ЗАО “Монлайн” – компании, которая специализируется на создании современных информационно-вычислительных систем, систем безопасности – считает, что определяющим фактором при выборе средств защиты информации является ее стоимость. Поскольку неразумно тратить на защиту средства большие, чем ее предполагаемая цена. Разумными считаются расходы в размере не более 10% стоимости информации. [5]

Информацию нужно защищать не только от несанкционированного доступа, но и от уничтожения. С этой целью в любой компании действует система резервного копирования данных. Специалисты в области информационной безопасности рекомендуют дополнять системы резервного копирования криптографическими модулями для защиты данных, размещаемых на внешних жестких дисках.

Выводы

По итогам данной статьи можно сказать, что криптографические методы защиты являются одним из лучших вариантов сокрытия информации на сегодняшний день.

При планировании защиты необходимо знать, кого и какая именно информация будет интересовать, какова ценность этой информации и каковы уязвимости системы хранения.

Система защиты должна быть комплексной. Стоит обеспечивать защиту сразу на трех уровнях: программном, программно-аппаратном и аппаратном.

В то же время система защиты информации должна быть гибкой и адаптированной. В этом главную роль играет

администрирование: регулярная смена паролей и ключей, строгий порядок их хранения, анализ журналов регистрации событий в системе, распределение полномочий пользователей в системе и другое.

Для шифрования информации использовать симметричные алгоритмы шифрования, для шифрования ключей использовать ассиметричные алгоритмы.

Для контроля целостности пользовательских данных использовать электронно-цифровую подпись.

Предусмотреть возможность реализации резервного копирования информации стандартными средствами операционных систем.

Система должна иметь простой и понятный интерфейс.

Список литературы

1. Саймон Сингх. Книга шифров. Тайная история шифров и их расшифровки. — АСТ, Астрель, 2007 г. — 446 с.
2. Использование шифрования в компаниях России: [электронный ресурс]. Режим доступа: http://habrahabr.ru/company/cybersafe/blog/220023/
3. Современная криптография: [электронный ресурс]. Режим доступа: http://www.osp.ru/cio/2006/08/2681235/
4. Стандарты сетевой защиты информации: [электронный ресурс]. Режим доступа: http://www.s-terra.com/solutions/standards/
5. Исследование “Средства защиты информации”: [электронный ресурс]. Режим доступа: http://www.itsec.ru/articles2/Oborandteh/issledovanie_sredstva_zashity