УДК: 621.396:004.77

ИНСТРУМЕНТЫ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СЕТЯХ

Павловская Кристина Каземировна, *студентка КГТУ им. И.Раззакова, Кыргызстан, г.Бишкек, пр. Мира 66, e-mail: kristi08.94@mail.ru*
Абдыллаева Гульнара Оморовна, *к.п.н., доцент, КГТУ им. И.Раззакова, Кыргызстан, 720044, г. Бишкек, пр. Мира 66, e-mail: g.abdyllaeva@mail.ru*

Цель статьи - защита личных прав и конфиденциальности информации в компьютерных сетях. Проблема отказоустойчивости сети и защиты данных является актуальной. Ведь не секрет, что многие фирмы на заре своей деятельности отдавали предпочтение наиболее дешевым и, зачастую, наименее надежным сетевым решениям. По данным анкетирования серьезные сбои в работе сетевого оборудования и программного обеспечения в большинстве фирм происходят не реже, чем один раз в месяц.

Ключевые слова: защита информации, компьютерные сети, данные, целостность, архивирование, вирусы, электронная подпись, криптография, несанкционированный доступ.

TOOLS FOR PROTECTING CONFIDENTIAL INFORMATION IN COMPUTER NETWORKS

Pavlovskaya Kristina Kazemirovna, *graduate student of IET under the KSTU named after I. Razzakov, Kyrgyz Republic, 720044 Mir Avenue 66, e-mail: kristi08.94@mail.ru*
Abdyllaeva Gulnara Omorovna, *PhD, Associate professor, KSTU named after I.Razzakov, Kyrgyzstan, 720044, Bishkek, Kyrgyzstan, e-mail: g.abdyllaeva@mail.ru*

The purpose of the article is the protection of personal rights and privacy of information in computer networks. The problem of network fault tolerance and data protection is topical. After all, it's no secret that many companies at the dawn of their activity preferred the cheapest and, often, the least reliable network solutions. According to the survey, serious disruptions in the operation of network equipment and software in most firms occur at least once a month.

Keywords: information protection, computer networks, data, integrity, archiving, viruses, electronic signature, cryptography, unauthorized access.

Не случайно, что защита данных в компьютерных сетях становится одной из самых острых проблем в современном мире. На сегодняшний день сформулировано три базовых принципа информационной безопасности, которая должна обеспечивать:

- целостность данных - защиту от сбоев, ведущих к потере информации, а также неавторизованного создания или уничтожения данных;
- конфиденциальность информации;
- ее доступность для всех авторизованных пользователей.

Следует также отметить, что отдельные сферы деятельности (банковские и финансовые институты, информационные сети, системы государственного управления, оборонные и специальные структуры) требуют специальных мер безопасности данных и предъявляют повышенные требования к надежности функционирования информационных систем, в соответствии с характером и важностью решаемых ими задач. В данной статье мы не будем затрагивать вопросы специальных систем безопасности, а остановимся на общих вопросах защиты информации в компьютерных сетях.

При рассмотрении проблем защиты данных в сети прежде всего возникает вопрос о классификации сбоев и нарушений прав доступа, которые могут привести к уничтожению или нежелательной модификации данных. Среди таких потенциальных "угроз" можно выделить:

1. Сбои оборудования:
- сбои кабельной системы;
- перебои электропитания;
- сбои дисковых систем;
- сбои систем архивации данных;
- сбои работы серверов, рабочих станций, сетевых карт и т. д.;

2. Потери информации из-за некорректной работы ПО:
- потеря или изменение данных при ошибках ПО;
- потери при заражении системы компьютерными вирусами;

3. Потери, связанные с несанкционированным доступом:
- несанкционированное копирование, уничтожение или подделка информации;
- ознакомление с конфиденциальной информацией, составляющей тайну, посторонних лиц;

4. Потери информации, связанные с неправильным хранением архивных данных.

5. Ошибки обслуживающего персонала и пользователей.
- случайное уничтожение или изменение данных;

- некорректное использование программного и аппаратного обеспечения, ведущее к уничтожению или изменению данных.

В зависимости от возможных видов нарушений работы сети (под нарушением работы мы также понимаем и несанкционированный доступ) многочисленные виды защиты информации объединяются в два основных класса:

- средства физической защиты, включающие средства защиты кабельной системы, систем электропитания, средства архивации, дисковые массивы и т. д.

- программные средства защиты, в том числе: антивирусные программы, системы разграничения полномочий, программные средства контроля доступа.

- административные меры защиты, включающие контроль доступа в помещения, разработку стратегии безопасности фирмы, планов действий в чрезвычайных ситуациях и т.д.

Следует отметить, что подобное деление достаточно условно, поскольку современные технологии развиваются в направлении сочетания программных и аппаратных средств защиты. Наибольшее распространение такие программно-аппаратные средства получили, в частности, в области контроля доступа, защиты от вирусов.

Системы архивирования и дублирования информации: Организация надежной и эффективной системы архивации данных является одной из важнейших задач по обеспечению сохранности информации в сети. В небольших сетях, где установлены один-два сервера, чаще всего применяется установка системы архивации непосредственно в свободные слоты серверов. В крупных корпоративных сетях наиболее предпочтительно организовать выделенный специализированный архивационный сервер.

Хранение архивной информации, представляющей особую ценность, должно быть организовано в специальном охраняемом помещении. Специалисты рекомендуют хранить дубликаты архивов наиболее ценных данных в другом здании, на случай пожара или стихийного бедствия. Для обеспечения восстановления данных при сбоях магнитных дисков в последнее время чаще всего применяются системы дисковых массивов - группы дисков, работающих как единое устройство, соответствующих стандарту RAID (Redundant Arrays of Inexpensive Disks).

Защита от компьютерных вирусов: Вряд ли найдется хотя бы один пользователь или администратор сети, который бы ни разу не сталкивался с компьютерными вирусами. По данным исследования, проведенного фирмой Creative Strategies Research, 64% из 451 опрошенного специалиста испытали "на себе" действие вирусов. На сегодняшний день дополнительно к тысячам уже известных вирусов появляется 100-150 новых штаммов ежемесячно. Наиболее распространенными методами защиты от вирусов по сей день остаются различные антивирусные программы.

Защита от несанкционированного доступа: Проблема защиты информации от несанкционированного доступа особо обострилась с широким распространением локальных и, особенно, глобальных компьютерных сетей. Необходимо также отметить, что зачастую ущерб наносится не из-за "злого умысла", а из-за элементарных ошибок пользователей, которые случайно портят или удаляют жизненно важные данные. В связи с этим, помимо контроля доступа, необходимым элементом защиты информации в компьютерных сетях является разграничение полномочий пользователей.

В компьютерных сетях при организации контроля доступа и разграничения полномочий пользователей чаще всего используются встроенные средства сетевых операционных систем.

Технические средства защиты информации - это системы охраны территорий и помещений с помощью экранирования машинных залов и организации контрольно-пропускных систем. Защита информации в сетях и вычислительных средствах с помощью технических средств реализуется на основе организации доступа к памяти с помощью: контроля доступа к различным уровням памяти компьютеров; блокировки данных и ввода ключей; выделение контрольных битов для записей с целью идентификации и др.

Для надёжной защиты информации и выявления случаев неправомочных действий проводится регистрация работы системы: создаются специальные дневники и протоколы, в

которых фиксируются все действия, имеющие отношение к защите информации в системе. Фиксируются время поступления заявки, её тип, имя пользователя и терминала, с которого инициализируется заявка. При отборе событий, подлежащих регистрации, необходимо иметь в виду, что с ростом количества регистрируемых событий затрудняется просмотр дневника и обнаружение попыток преодоления защиты. В этом случае можно применять программный анализ и фиксировать сомнительные события. Используются также специальные программы для тестирования системы защиты. Периодически или в случайно выбранные моменты времени они проверяют работоспособность аппаратных и программных средств защиты.

К отдельной группе мер по обеспечению сохранности информации и выявлению несанкционированных запросов относятся программы обнаружения нарушений в режиме реального времени. Программы данной группы формируют специальный сигнал при регистрации действий, которые могут привести к неправомерным действиям по отношению к защищаемой информации. Сигнал может содержать информацию о характере нарушения, месте его возникновения и другие характеристики. Кроме того, программы могут запретить доступ к защищаемой информации или симулировать такой режим работы (например, моментальная загрузка устройств ввода-вывода), который позволит выявить нарушителя и задержать его соответствующей службой.

Один из распространённых способов защиты - явное указание секретности выводимой информации. В системах, поддерживающих несколько уровней секретности, вывод на экран терминала или печатающего устройства любой единицы информации (например, файла, записи и таблицы) сопровождается специальным грифом с указанием уровня секретности. Это требование реализуется с помощью соответствующих программных средств.

Одним из удачных примеров создания комплексного решения для контроля доступа в открытых системах, основанного как на программных, так и на аппаратных средствах защиты, стала система Kerberos. В основе этой схемы авторизации лежат три компонента:

- База данных, содержащая информацию по всем сетевым ресурсам, пользователям, паролям, шифровальным ключам и т.д.

- Авторизационный сервер (authentication server), обрабатывающий все запросы пользователей на предмет получения того или иного вида сетевых услуг. Авторизационный сервер, получая запрос от пользователя, обращается к базе данных и определяет, имеет ли пользователь право на совершение данной операции. Примечательно, что пароли пользователей по сети не передаются, что также повышает степень защиты информации.

- Ticket-granting server (сервер выдачи разрешений) получает от авторизационного сервера "пропуск", содержащий имя пользователя и его сетевой адрес, время запроса и ряд других параметров, а также уникальный сессионный ключ. Пакет, содержащий "пропуск", передается также в зашифрованном по алгоритму DES виде. После получения и расшифровки "пропуска" сервер выдачи разрешений проверяет запрос и сравнивает ключи и затем дает "добро" на использование сетевой аппаратуры или программ.

Инструменты обеспечения безопасности. Криптография.

Для обеспечения секретности применяется шифрование, или криптография, позволяющая трансформировать данные в зашифрованную форму, из которой извлечь исходную информацию можно только при наличии ключа.

Системам шифрования столько же лет, сколько письменному обмену информацией.

“Криптография” в переводе с греческого языка означает “тайнопись”, что вполне отражает её первоначальное предназначение.

Классической задачей криптографии является обратимое преобразование некоторого понятного исходного текста в кажущуюся случайной последовательность некоторых знаков, называемую шифртекстом или криптограммой.

В основе шифрования лежат два основных понятия: алгоритм и ключ. Алгоритм - это способ закодировать исходный текст, в результате чего получается зашифрованное послание. Зашифрованное послание может быть интерпретировано только с помощью ключа.

Электронная подпись

Если послание, безопасность которого мы хотим обеспечить, должным образом зашифровано, всё равно остаётся возможность модификации исходного сообщения или подмены этого сообщения другим. Одним из путей решения этой проблемы является передача пользователем получателю краткого представления передаваемого сообщения. Подобное краткое представление называют контрольной суммой, или дайджестом сообщения.

Однако при использовании контрольных сумм возникает проблема передачи их получателю. Одним из возможных путей её решения является включение контрольной суммы в так называемую электронную подпись.

При помощи электронной подписи получатель может убедиться в том, что полученное им сообщение послано не сторонним лицом, а имеющим определённые права отправителем. Электронные подписи создаются шифрованием контрольной суммы и дополнительной информации при помощи личного ключа отправителя. Таким образом, кто угодно может расшифровать подпись, используя открытый ключ, но корректно создать подпись может только владелец личного ключа. Для защиты от перехвата и повторного использования подпись включает в себя уникальное число - порядковый номер.

Аутентификация

Аутентификация является одним из самых важных компонентов организации защиты информации в сети. Прежде чем пользователю будет предоставлено право получить тот или иной ресурс, необходимо убедиться, что он действительно тот, за кого себя выдаёт.

При получении запроса на использование ресурса от имени какого-либо пользователя сервер, предоставляющий данный ресурс, передаёт управление серверу аутентификации. После получения положительного ответа сервера аутентификации пользователю предоставляется запрашиваемый ресурс.

При аутентификации используется, как правило, принцип, получивший название “что он знает”, - пользователь знает некоторое секретное слово, которое он посылает серверу аутентификации в ответ на его запрос. Одной из схем аутентификации является использование стандартных паролей.

Защита сетей

В последнее время корпоративные сети всё чаще включаются в Интернет или даже используют его в качестве своей основы. Учитывая то, какой урон может принести незаконное вторжение в корпоративную сеть, необходимо выработать методы защиты. Для защиты корпоративных информационных сетей используются брандмауэры. Брандмауэры - это система или комбинация систем, позволяющие разделить сеть на две или более частей и реализовать набор правил, определяющих условия прохождения пакетов из одной части в другую. Как правило, эта граница проводится между локальной сетью предприятия и INTERNETOM, хотя её можно провести и внутри. Однако защищать отдельные компьютеры невыгодно, поэтому обычно защищают всю сеть. Брандмауэр пропускает через себя весь трафик и для каждого проходящего пакета принимает решение - пропускать его или отбросить. Для того чтобы брандмауэр мог принимать эти решения, для него определяется набор правил.

Брандмауэр может быть реализован как аппаратными средствами (то есть как отдельное физическое устройство), так и в виде специальной программы, запущенной на компьютере.

Выводы: любой пользователь в защите личных прав, который хочет защитить свои ресурсы самым надежным образом, должен применять комплексный подход. Кроме вышеназванных, понадобится система, которая будет осуществлять обнаружение вторжений, предотвращать их, не допускать утечек конфиденциальной информации. Желательно использование средств мониторинга сетей, анализа и моделирования информационных потоков, качественных антивирусных программ, не нужно забывать об архивировании и

дублировании данных, резервном копировании, анализаторах протоколов, организационных и административных мерах, которые бы помогли предотвратить физический доступ посторонних к ее информации.

Список литературы

1. Безопасность компьютерных коммуникаций Warwick Ford. Принципы, стандартные протоколы и методы // PTR Prentice Hall, 1994, 500p.

2. Регис Дж. Бейтс Физическая защита // в аварийном восстановлении для ЛВС, 1994, McGraw-Hill, Inc, pp. 44-65

3. М. Рааб (M.Raab) Защита сетей: наконец-то в центре внимания // Компьютеруорлд Москва, 1994, №29, с. 18

4. Д.Векслер (Дж. Векслер) Наконец-то надежно обеспечена защита данных в радиосеиях // Компьютеруорлд Москва, 1994, N17, сс. 13-14

5. Проблемы финансов / банковской безопасности: обзор за 1994 год // Доклады Datapro по автоматизации банковской деятельности McGraw-Hill Inc., февраль 1995 г., стр. 101-108

6. Датапро на CD-ROM Communications Analyst, 1994, октябрь.

7. С.В. Сухова. Система безопасности NetWare // "Cemu", 1995, N4, сс. 60-70