



КИБЕРБЕЗОПАСНОСТИ — ЭТО СЛАБЫЕ МЕСТА В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Аррыкова Гульджемал Керимназаровна

Старший преподаватель, Международного университета нефти и газа имени
Ягшыгелди Какаева
г. Ашхабад Туркменистан

Гелдиев Сердар Отузбаевич

Преподаватель, Международного университета нефти и газа имени
Ягшыгелди Какаева
г. Ашхабад Туркменистан

Аширова Хатыджа Мердановна

Студент, Международного университета нефти и газа имени Ягшыгелди
Какаева
г. Ашхабад Туркменистан

Чуриев Мейлис Мергенович

Студент, Международного университета нефти и газа имени Ягшыгелди
Какаева
г. Ашхабад Туркменистан

После окончания работы обрабатываемая информация не всегда полностью удаляется. Часть данных, оставшаяся на дисках и в оперативной памяти, собирается и обрабатывается. Правило противодействия. Заполнение памяти нулями или единицами, перезапись информации в другое место.

Недокументированная производителем программного обеспечения точка входа в программный модуль используется для активного воздействия на эту программу.

Правило противодействия. При приемке программного обеспечения необходимо производить анализ программ с целью обнаружения люка.

Вирусы. Программа, которая заражает другие программы путем включения в них своих кодов, при этом зараженная программа имеет способность дальнейшего размножения. Вирусы в основном разрушают программное обеспечение.

Правило противодействия. Использование антивирусного программного обеспечения и специальных программ. Более подробно они будут описаны ниже.

«Жадные» программы. Программы, монопольно захватывающие ресурсы системы, не давая другим программам его использования. Правило противодействия. Ограничение времени исполнения программ.

Методы и средства защиты информации в компьютерных сетях. Накопленный опыт технологий защиты информации в компьютерных сетях показывает, что только комплексный подход к защите информации может обеспечить современные требования безопасности.

Комплексный подход подразумевает комплексное развитие всех методов и средств защиты.

Рассмотрим кратко основные методы и средства обеспечения безопасности информации в компьютерных сетях.

Методы защиты информации делятся:

- на препятствия;
- управление доступом;
- маскировка;
- регламентация;
- принуждение;
- побуждение.

Препятствие — метод физического преграждения пути злоумышленнику к защищаемой информации (компьютеру, сетевому оборудованию)

Управление доступом — метод защиты информации регулированием использования всех ресурсов системы. Управление доступом включает следующие функции защиты:

- идентификация пользователей, персонала и ресурсов системы путем присвоения каждому объекту персонального идентификатора;
- опознавание объекта или субъекта по предъявляемому им идентификатору;
- проверка полномочий на запрашиваемые ресурсы;
- регистрация обращений к защищаемым ресурсам;
- реагирование при попытках несанкционированных действий

Маскировка — метод защиты информации с помощью ее криптографического закрытия (шифрования). В настоящее время этот метод является наиболее надежным. Известны три основных алгоритма: алгоритм DES, современный алгоритм Clipper (Capston) и так называемая общественная инициатива — алгоритм PGP.

Алгоритм шифрования DES (Data Encryption Standard) был разработан в начале 1970-х гг. Алгоритм шифрования был реализован в виде интегральной схемы с длиной ключа в 64 символа (56 символов используются непосредственно для алгоритма шифрования и 8 для обнаружения ошибок).

Расчет алгоритмов в то время показывал, что ключ шифрования может иметь 72 квадриллиона комбинаций. Алгоритм DES был принят в США в качестве федерального стандарта обработки информации в 1977 г., а в середине 1980-х был утвержден как между народный стандарт, который каждые пять лет проходит процедуру подтверждения. Для оценки уровня защиты информации аналитики приводят такие факты: современный компьютер стоимостью 1 млн дол. раскроет шифр за 7 часов, стоимостью 10 млн дол. — за 20 минут, 100 млн дол. — за 2 минуты. Агентство национальной безопасности США имеет такой компьютер.

Новый метод шифрования информации — технология Clipper — разработан агентством национальной безопасности США для защиты от прослушивания телефонных разговоров.

Для защиты данных этот метод носит название Capston. В основе метода положен принцип двух ключей-микросхем, обеспечивающих шифрование информации со скоростью до 1 гигабита в секунду. Пользователи получают ключи в двух пунктах, управляемых правительственными органами или частными концернами. Система ключей состоит из двух интегральных схем Clipper chip и Capston chip и алгоритма шифрования SKIPJACK. Алгоритм шифрования шифрует символьные блоки данных с помощью 80-символьного ключа в 32 прохода. Он в 16 миллионов раз мощнее алгоритма DES и считается, только через несколько десятков лет компьютеры стоимостью 100 млн дол. смогут расшифровывать информацию за 2 минуты. Для сети Интернет разработан специальный протокол шифрования SKIP (Simple Key management for Internet Protocol), управляющий шифрованием потоков информации. Следует отметить, что в настоящее время федеральные власти США запрещают экспорт протокола SKIP, поэтому во многих странах предпринимаются попытки создания его аналога.

Криптографические программные средства PGP (Pretty Good Privacy) были разработаны в 1991 году американским программистом Ф. Циммерманном для зашифровки сообщений электронной почты. Программа PGP свободна для доступа в Интернете и может быть установлена на любой компьютер. Принцип работы программы PGP основан на использовании двух программ-ключей: одной у отправителя, а другой у получателя. Программы-ключи защищены не паролями, а шифровой фразой. Расшифровать сообщение можно, только используя два ключа. Программа PGP использует сложный математический алгоритм, что вместе с принципом использования двух ключей делает дешифрацию практически невозможной. Появление программ PGP вызвало скандал в правоохранительных кругах США, так как они лишают возможности контроля за информацией. Следует отметить то, что криптографические алгоритмы широко используются для защиты электронной цифровой подписи.

Более полную информацию о криптографических методах можно получить на сайте www.cripto.com или www.confident.ru

Регламентация — метод защиты информации, создающий такие условия автоматизированной обработки, хранения и передачи защищаемой информации, при которых возможности несанкционированного доступа к ней сводился бы к минимуму.

Принуждение — такой метод защиты информации, при котором пользователи и администраторы сети вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности.

Побуждение — метод защиты, который побуждает пользователей и администраторов сети не нарушать установленных моральных и этических норм.

Средства защиты информации делятся на следующие группы:

- технические средства;
- программные средства;
- организационные средства;
- морально-этические средства;
- законодательные средства.

Защита информации в сети Интернет. Несмотря на предпринимаемые меры, проблема несанкционированного доступа к ресурсам Интернета до конца не решена, хотя и сформулирован ряд положений по обеспечению безопасности обработки информации.

Авторизация доступа к Интернет предназначена прежде всего для учета использования ее ресурсов и оплаты услуг. Поэтому, как правило, авторизация доступа осуществляется провайдерами и предназначена исключительно для коммерческого использования. Различные провайдеры предоставляют своим клиентам различную степень свободы. Так, например, при выделенном TCP/IP подключении пользователь оказывается привязанным к конкретному географическому адресу.

При подключении по коммутируемым каналам связи выход в сети может быть осуществлен с любого телефонного аппарата. Кроме этого, конкуренция провайдеров на рынке привела к новому виду предоставления услуг — гостевому, позволяющему работать в сети без регистрации и оплаты. В этом случае сетевой адрес назначается провайдером динамически и проконтролировать такого пользователя, если он занимается хакерской деятельностью, является достаточно сложной задачей. Единственной возможностью является анализ регулярных попыток пользователя получить доступ к ресурсам, которые не пользуются популярностью у других абонентов.

Основным средством защиты сети Интернет от несанкционированного доступа в настоящее время является файрволл. Файрволлы контролируют информационные потоки между локальными сетями, причем уровень контроля определяется в первую очередь сферой интересов компании, структурой локальной сети и целями, ради которых локальная сеть подключается к Интернету.

Система файрволл обеспечивает защиту программного обеспечения сервера и пользователей от доступа без соответствующей авторизации, но в то же время не препятствует нормальной работе штатных протоколов (электронная почта, ftp, WWW и др.).

Во многих организациях файрволл используется для хранения данных с открытым доступом, например, информация о продуктах и услугах, сообщения об ошибках и т.д. Дополнительный контур защиты, организованный с помощью файрволла, реализуется за счет объединения точек контроля доступа и обеспечения безопасности в одном и том же месте, как аппаратно, так и программно.

Следует отметить, что системы класса файрволл не в состоянии обеспечить защиту от вирусов и червей, они также беззащитны перед атакой, когда в поражаемую систему под видом сетевой почты копируется какая-либо программа, которая после открытия почтового ящика запускается на выполнение.

Существует метод защиты локальной сети, который используется для защиты сетей крупных банков в США при их подключении к Интернету, когда блокируются все внешние потоки информации и в локальную сеть поступают лишь копии разрешенных сообщений. В этом случае между локальной сетью и сетью Интернет нет точек непосредственного соприкосновения, а весь поток информации обрабатывается прохi-сервером. В случае если с любого компьютера локальной сети поступает запрос к ресурсам Интернета, то прохi-сервер проверяет у пользователя права доступа к Интернету. В ходе сеанса связи система безопасности регистрирует всех пользователей внешней связью, имена пересылаемых файлов, все сообщения копируются.

Как правило, для ограничения доступа внешних пользователей к локальной сети составляются таблицы контроля доступа, так называемые access control lists, которые используются маршрутизаторами при получении пакетов. Отметим, что создавать такие таблицы довольно сложно, а их просмотр снижает производительность сети.

По оценке специалистов системы безопасности, установленные на маршрутизаторах, менее надежны, чем основанные на применении файрволлов и прохi-серверов. С другой стороны, сами файрволлы и прохi-сервера могут быть атакованы взломщиками. Поэтому оптимальным является комбинированный подход: маршрутизатор отвергает нежелательные запросы доступа и передает все остальные запросы файрволлу и далее прохi-серверу.