# Практическое построение системы безопасности информационных ресурсов предприятия

Луговой Д.А., Васильева М.А., учебный центр "Трайтек", г.Саратов

Ведение современного бизнеса невозможно без применения новейших компьютерных технологий. Большой объем информации, в том числе конфиденциальная и критичная информация, современной компании хранится и обрабатывается на компьютерах при помощи информационных технологий (ИТ). В связи с этим ИТ становятся все более критичным ресурсом для ведения непрерывного бизнеса компании, а стабильная работа автоматизированной системы является основным фактором его успешности.

Устойчивость работы ИТ можно обеспечить при помощи построения системы информационной безопасности. Когда речь заходит об обеспечении безопасности любого предприятия, то первое с чего начинают - это физическая безопасность. Системы разграничения доступа, турникеты, системы пожарной и охранной сигнализации, видео наблюдения устанавливаются в первую очередь. Информационная система это тоже своего рода здание, только виртуальное, которое необходимо защищать от посягательства преступников. Преступники в данном случае действуют на расстоянии и практически безнаказанно проникают в корпоративные сети. Использовать для защиты виртуального здания можно механизмы физической безопасности, но спроектированные с учетом особенностей информационных технологий. Например, турникеты, охранники в реальном пространстве - это межсетевые экраны, антивирусные программы, или системы идентификации - в виртуальном. Ниже обсуждаются вопросы построения именно компьютерной безопасности.

Обобщенная схема информационных систем в организациях, которые занимаются геологической разведкой, может иметь структуру, приведенную на рис 1.

Вопросы защиты в данном случае можно разделить на следующие группы.

1. Защита корпоративной сети, подключенной к Интернет и физически расположенной в основном офисе:

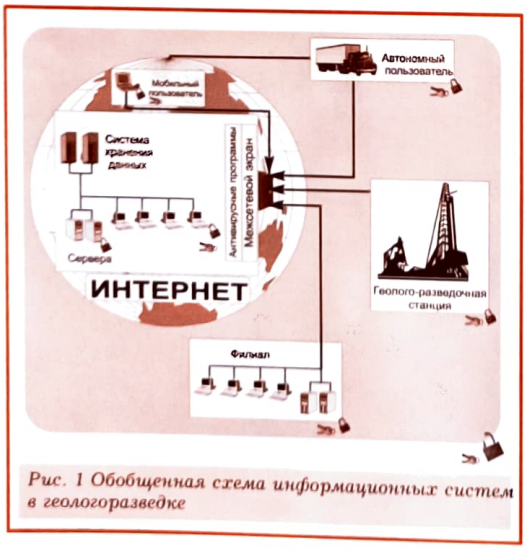


*Рис. 1 Обобщенная схема информационных систем в геологоразведке*

- защита внешнего периметра сети от проникновения;
- система установления подлинности пользователя и разграничение доступа;
- обеспечение безопасного хранения баз данных с важной информацией.

2. Защита каналов передачи данных:
- между филиалами;
- стационарными станциями и основным предприятием;
- мобильными станциями и основным офисом;
- обеспечение безопасного доступа стационарных и мобильных пользователей (топ-менеджеров) к определенным сетевым ресурсам предприятия.

Рассмотрим данные составляющие более подробно.

**Защита корпоративной сети от несанкционированного доступа извне**.

*Защита внешнего периметра сети от проникновения*

Надежная система безопасности нашего виртуального здания возможна при наличии нескольких составляющих: аналога контрольно-пропускных систем (межсетевые экраны, антивирусные программы); "систем пожарной безопасности" (аппаратные и программные средства резервного копирования); "сейфов" для хранения конфиденциальной информации (системы шифрования баз данных).

Начнем описание **с межсетевых экранов (МЭ) и антивирусных программ.** Каждый раз, выходя в Интернет, мы получаем возможность пользоваться всеми ресурсами глобальной компьютерной сети, но одновременно предоставляем гипотетическим злоумышленникам потенциальную возможность воспользоваться нашими собственными ресурсами.

В конце января этого года появилась новый вредоносный сетевой вирус-"червь" "Novarg" (также известный как "Mydoom"), который всего за несколько часов существования успел вызвать глобальную эпидемию в мировой компьютерной сети. "Novarg" весьма опасен. Во-первых, червь устанавливает на зараженный компьютер модуль, который может позднее использоваться злоумышленниками для рассылки спама или новых версий вредоносной программы. Во-вторых, на компьютер внедряется программа, которая позволяет вирусописателям полностью контролировать зараженную машину. С ее помощью можно похищать, удалять, изменять данные, устанавливать программы и др. В-третьих, в "Novarg" заложена функция организации DoS-атаки на сайт "www.microsoft.com.

На рынке существует множество готовых устройств и программ, реализующих функцию МЭ, а также, есть специализированные программы на основе бесплатных ОС Linux или FreeBSD, из которых опытный пользователь может самостоятельно собрать МЭ.

В России наибольшую известность получили МЭ компании CISCO и Checkpoint.

Согласно документам компании CISCO МЭ

Табл. 1 Особенности межсетевых экранов

| Тип межсетевого экрана | Принцип работы | Достоинства | Недостатки |
|---|---|---|---|
| Экранирующие маршрутизаторы (брандмауэры с фильтрацией пакетов) | Фильтрация пакетов осуществляется в соответствии с IP- заголовком пакета по критерию: то, что явно не запрещено, является разрешенным. Анализируемой информацией является:<br>- адрес отправителя;<br>- адрес получателя;<br>- информация о приложении или протоколе;<br>- номер порта источника;<br>- номер порта получателя. | • Низкая стоимость<br>• Минимальное влияние на производительность сети<br>• Простота конфигурации и установки<br>• Прозрачность для программного обеспечения | • Уязвимость механизма защиты для различных видов сетевых атак, таких как подделка исходных адресов пакетов, несанкционированное изменение содержимого пакетов<br>• Отсутствие в ряде продуктов поддержки журнала регистрации событий и средств аудита |
| Экранирующий шлюз (ЭШ) | Информационный обмен происходит через хост-бастион, установленный между внутренней и внешней сетями, который принимает решения о возможности маршрутизации трафика. ЭШ бывают двух типов: сеансового и прикладного уровня | • Отсутствие сквозного прохождения пакетов в случае сбоев<br>• Усиленные, по сравнению с ЭМ, механизмы защиты, позволяющие использовать дополнительные средства аутентификации, как программные, так и аппаратные<br>• Использование процедуры трансляции адресов, позволяющей скрытие адресов хостов закрытой сети | • Использование только мощных хостов-бастионов из-за большого объема вычислений<br>• Отсутствие "прозрачности" из-за того, что ЭШ вносят задержки в процесс передачи и требуют от пользователя процедур аутентификации |
| Экранирующие подсети (ЭП) | Создается изолированная подсеть, расположенная между внутренней и открытой сетями.<br>• Сообщения из открытой сети обрабатываются прикладным шлюзом и попадают в ЭП. После успешного прохождения контроля в ЭП они попадают в закрытую сеть.<br>Запросы из закрытой сети обрабатываются через ЭП аналогично. Фильтрование осуществляется из принципа: то, что не разрешено, является запрещенным | • Возможность скрытия адреса внутренней сети<br>• Увеличение надежности защиты<br>• Возможность создания большого трафика между внутренней и открытой сетями при использовании нескольких хостов-бастионов в ЭП<br>• "прозрачность" работы для любых сетевых служб и любой структуры внутренней сети | • Использование только мощных хостов-бастионов из-за большого объема вычислений<br>• Техническое обслуживание (установка, конфигурирование) может осуществляться только специалистами |

- это маршрутизатор или сервер доступа или множество маршрутизаторов или серверов доступа, работающих как буфер между соединенными открытыми сетями и защищенной сетью. МЭ использует списки доступа или иные методы для обеспечения безопасности защищаемой сети. При этом МЭ обычно имеет три интерфейса, один соединяется с внешней сетью, второй с защищаемой сетью, а третий используется в качестве так называемой "демилитаризованной зоны".

МЭ делятся на три типа: пакетные фильтры; экранирующий шлюз и экранирующие подсети.

Cisco Secure PIX относится к третьему типу. Смысл данного типа сводится к следующему - данные фильтры записывают и сохраняют информацию о каждой сессии, проходящей через МЭ. Каждый раз, когда устанавливается IP соединение, информация собирается в специальных таблицах. Данная таблица содержит информацию об адресах источника и получателя, номера портов, информацию о TCP последовательностях и дополнительные флаги TCP/UDP соединений. Как только сессия установилась через МЭ, собирается указанная таблица и все последующие пакеты будут анализироваться исходя их данные таблицы.

МЭ от компании Checkpoint можно определить, как мощный программный МЭ с возможностью распределенной установки на сети. Хотя это не совсем точно, существует аппаратно-программный МЭ - плод совместной работы компаний Checkpoint и Nokia.

При этом необходимо отметить, что компания Checkpoint продвигает не просто МЭ, а целую архитектуру SVN (Secure Virtual Network), ключевым компонентом которой и является Checkpoint VPN-1/Firewall-1.

По результатам анализа российского рынка в табл.2 приведены сравнительные характеристики современных межсетевых экранов.

События уже текущего года еще раз подтверждают, что компьютерные вирусы перестали быть злыми шутками студентов, а все чаще используются как "информационное оружие массового поражения".

Ранее предполагалось, что каждый пользователь должен сам заботиться о защите своего компьютера от вирусов, программ типа "троянский конь" и других разрушающих программ. При этом он должен был сам заниматься установлением программного средства, отслеживать изменения в новых версиях и проводить обновление антивирусной базы. Однако наша практика показала, что такой подход ошибочен. Не всякий пользователь умеет

Табл. 2 Сравнительные характеристики современных межсетевых экранов

| Продукт | Тип | Платформа | Компания | Особенности |
|---|---|---|---|---|
| Firewall-1 | Комплексный межсетевой экран | Intel x86, Sun Sparc и др. | Check Point Software Technologies | Обеспечивает защиту от хакерских нападений типа address-spoofing (подделка адресов пакетов) и представляет комбинацию средств защиты сетевого и прикладного уровней. |
| Firewall-1/ VPN-1 | Комплексный межсетевой экран | Intel x86, Sun Sparc и др. | Check Point Software Technologies | Представляет открытый интерфейс приложения OPSEC API. Обеспечивает:<br>- выявление компьютерных вирусов;<br>- сканирование URL;<br>- блокирование Java и ActiveX;<br>- поддержку протокола SMTP;<br>- фильтрацию HTTP;<br>- обработку протокола FTP |
| TIS Firewall Toolkit | Набор программ для создания и управления системами firewall | BSD UNIX | Trusted Information Systems | Распространяется в исходном коде, все модули написаны на языке С.<br>Набор предназначен для программистов- экспертов. |
| Gauntlet Internet Firewall | Экранирующий шлюз прикладного уровня | UNIX, Secured BSD | Trusted Information Systems | Поддерживает сервисы: электронная почта, Web-сервис, терминальные сервисы и др.<br>Возможности: шифрование на сетевом уровне, защита от хакерских нападений типа address-spoofing, защита от попыток изменения маршрутизации. |
| FireWall/ Plus | Мульти-протокольный межсетевой экран | Различные аппаратные платформы | Network-1 Software and Technology | Контроль реализован на уровне кадров, пакетов, каналов и приложений (для каждого протокола). Позволяет работать с более чем 390 протоколами, дает возможность описать любые условия фильтрации для последующей работы. |

хорошо работать с ПЭВМ, а некоторые преднамеренно выключают антивирусное ПО, заявляя, что оно мешает работе компьютера (замедляет работу). Поэтому сейчас на первое место вышли именно **корпоративные версии антивирусных программ**, позволяющие управлять всеми компьютерами компании с одного места - сервера отдела безопасности, проводить централизованное обновление антивирусной базы (даже если сам пользователь об этом не знает), оперативно отслеживать работоспособность антивирусной программы.

В настоящее время можно выделить много компаний, продукция которых работает в качестве корпоративного антивируса. Можно отметить продукты Kaspersky Corporate Suite, антивирус от Trend Micro, Mac Cafi, Norton AntiVirus Corporate Edition. Поскольку традиционных антивирусных средств уже недостаточно для обеспечения надежной защиты от внешних угроз, в предложении почти всех антивирусных компаний присутствуют комплекс фильтрации спама Kaspersky Anti-Spam, средства фильтрации контента и трафика Web от "Лаборатории Касперского", Symantec, TrendMicro и Cobion.

При выборе корпоративного антивируса целесообразно придерживаться следующих правил:

- возможность обнаружения вирусов;
- возможность обнаружения деструктивного кода типа "троянский конь", ActiveX, Java;
- готовность быстрого реагирования на появление новых видов угроз;
- обслуживание и поддержка;
- исчерпывающий список защищаемых точек возможного проникновения вирусов; управляемость;
- управление антивирусной защитой удаленных пользователей;
- централизованное уведомление;
- производительность системы;
- удаленное администрирование;
- автоматическое распространение и обновление.

*Системы идентификации пользователя.*

Свыше 80% нарушений происходит внутри компании. Забыть о паролях и при этом повысить защищенность сети и удобство работы позволяет использование электронных ключей или смарт-карт. Электронные ключи имеют небольшой размер, легко размещаются на связке с ключам. На одном ключе может храниться несколько разных паролей, для доступа к разным ресурсам. Вы можете быть уверены, что никто, кроме зарегистрированных пользователей не сможет получить доступ к важной информации. Одна из задач, которую возможно решить при помощи смарт-карт, и usb-ключей - это безопасный доступ к внутренней информации компании удаленных пользователей, что особенно актуально для топ-менеджеров компании. Топ-менеджеры, находясь в командировках, имеют возможность безопасно работать с базой данных своей компании, постоянно быть в курсе корпоративных новостей, безбоязненно использовать свежую, актуальную корпоративную информацию. Как показала практика, большой популярностью пользуются средства аутентификации компании Aladdin, usb-ключи, смарт-карты. В декабре 2003 года eToken был признан Советом учредителей Национальной премии по безопасности "лучшим продуктом по безопасности". Согласно прогнозам исследовательской компании IDC, к 2004 году рынок средств ЗА (аутентификация, авторизация, администрирование) будет занимать около 2/3 всего сектора информационной безопасности при среднегодовом росте сектора в 28%.

*Обеспечение сохранности данных в сети* - это следующая из важнейших задач для успешного функционирования ИС предприятия. Именно из-за выхода из строя систем хранения информации, по данным корпорации Intel происходит 55% простоев серверов корпоративных сетей. Одним из наиболее распространенных и эффективных средств быстрого восстановления утерянных данных является организация системы резервного копирования.

На исследование структуры верхней части земной коры при геологоразведке уходит много времени, много ресурсов: материальных, человеческих. Информация, обрабатываемая в данной отрасли, долгое время остается актуальной.

Поэтому в случае чрезвычайной ситуации, при которой данные могут быть утеряны, необходимо иметь возможности их скорейшего восстановления. Одним из наиболее распространенных и эффективных средств быстрого восстановления утерянных данных является организация системы резервного копирования.

Материалов, посвященных хранению данных, существует много, есть даже отдельные издания, специализирующиеся на этой тематике, и данный номер журнала тоже посвящен ей. Поэтому мы намеренно не будем углубляться в технологии построения систем резервного копирования, в рассмотрение и сравнительный анализ соответствующих продуктов и решений, а остановимся на рекомендациях для системных администраторов, при построении более эффективной системы хранения данных:

- необходимо избегать концентрации банка данных в том же месте, где находится офис предприятия, и хранятся основные данные;
- необходимо регулярно и полностью проверять на работоспособность удаленные резервные центры;
- необходимо документировать конфигурацию систем, а также процедуру восстановления данных;
- необходимо беречь эту документацию, как и сами данные;
- необходимо знать, какие системы являются наиболее критичными для бизнеса - если бизнес без какой-то системы находится под угрозой существования, данную систему нужно защищать в первую очередь;
- необходимо приглашать профессиональных консультантов для организации систем резервного копирования;
- необходимо знать, где находятся все носители и насколько они стары - если лента слишком долго используется, данные с нее могут не восстановиться;
- необходимо помнить, что восстановление данных и приложений на оборудование, отличное от того, с которого они копировались, может привести к серьезным проблемам в дальнейшей работе.

На наш взгляд интегрированное решение по резервному копированию должно удовлетворять следующим требованиям:

- поддержка различных серверных и клиентских платформ (в нашем случае Novell Netware, Silicon Graphics Irix, MS DOS, Windows 3.1, Windows 95, Windows NT Workstation);
- размещение данных: локальное и удаленное;
- большой размер сохраняемых файлов;
- высокая скорость записи;
- широкий спектр услуг резервного копирования/восстановления;
- развитые средства администрирования;
- надежность, простота и удобство в использовании;
- возможность наращивания функциональности по мере развития сети (поддержка СУБД, интеграция с системами миграции информации, поддержка средств коллективной работы);
- поддержка широкого спектра носителей для копирования;
- приемлемое соотношение функциональность/стоимость.

В качестве наиболее интересных решений хотелось бы отметить системы резервного копирования PIX, Check point, HP.

**Защита каналов передачи данных.**

Если еще раз посмотрим на рис.1, то увидим, что в системе обмена информацией в геологоразведочной области, большое значение имеет передача, и получение информации с мобильных станций. Безопасные коммуникации между удаленными филиалами компании.

Дело в том, что передача данных в Интернете похожа на передачу информации на почтовых открытках без конверта - каждый заинтересованный почтовый работник может прочитать и даже добавить что-нибудь на эту открытку. Любой человек может послать открытку от имени другого человека.

Внедрение VPN позволит объединить информационные ресурсы территориально разделенных подразделений и централизовать управление бизнесом, позволит организовать безопасное получение информации мобильными пользователями из баз данных предприятий. Передача данных при помощи виртуальных частных сетей с применением средств криптографии похожа на упаковку открытки в конверт, его запечатывание и подписывание. Таким образом, вы можете гарантировать, что никто не читал информацию в конверте, никто не изменил информацию в нем, подпись на конверте гарантирует личность отправителя. А главное, виртуальные сети обеспечивают существенную экономию затрат по сравнению с содержанием собственной сети глобального масштаба. Однако при этом надо помнить, что внедрение решений на основе VPN может привести к снижению производительности и потребовать значительных начальных затрат. Поэтому решение вопроса о выборе или альтернативного решения требует тщательного анализа. Таким образом, современные решения по информационной безопасности дают еще и новые возможности ведения бизнеса.

В качестве компаний-производителей программ для реализации виртуальных частных сетей, можно назвать Cisco, Nokia/Check Point, Nortel. Среди российских систем хотелось бы отметить: "VipNet" компании "Инфотекс", "Континент" компании "Информзащита", "Застава" криптон компании "Элвис плюс".

**Заключение**

Защищать данные, безусловно, надо. В первую очередь - критически важные. Возможно, следует задуматься об автоматизации защиты хотя бы ключевых систем. Средства для этого есть. Есть и возможность выбрать то или иное решение, исходя из своих потребностей. Построение системы безопасности позволяет сделать автоматизированную систему компании более стабильной и эффективной, сэкономить деньги и открыть новые возможности для бизнеса!