ЗАЩИТА ИНФОРМАЦИИ В ЭПОХУ INTERNET

Александр ТУРСКИЙ, менеджер по продуктам защиты информации ОАО "ЭЛВИС+"
Банковское дело в Москве №12/1999

Быстрое развитие современных телекоммуникационных систем, в частности Internet, поднимает множество вопросов по информационной безопасности. Остановимся на двух из них:
1. Как защищать конфиденциальную информацию, передаваемую между отдельными офисами, а также обеспечить безопасный доступ удаленных сотрудников к информационным ресурсам банка?
2. Насколько опасна возрастающая интеграция банковских коммуникационных структур с Internet?

КАК ЗАЩИТИТЬ ПЕРЕДАВАЕМУЮ ПО СЕТЯМ ИНФОРМАЦИЮ?

Исторически большинство вопросов защиты информации в банках решалось контролем физического доступа сотрудников к определенным информационным ресурсам (компьютерам, принтерам, документам). Упомянутые выше два вопроса уже не могут быть решены таким подходом, поскольку:
- невозможно обеспечить физический контроль за линиями связи, лежащими вне стен банка;
- атака может осуществляться из любой точки планеты;
- спектр возможных атак на информацию чрезвычайно широк:
* нарушение конфиденциальности передаваемой информации;
* нарушение целостности - изменение информации, ее повторение или уничтожение;
* нарушение аутентичности - подделка авторства информации;
- отказ отправителя от факта отправки/авторства информации;
- атакующий может получить контроль над внутренними ресурсами банка, блокировать каналы, осуществлять комплексные атаки;
- факт осуществления атаки может остаться неизвестным владельцам информации, а последствия атаки могут проявиться существенно позже.

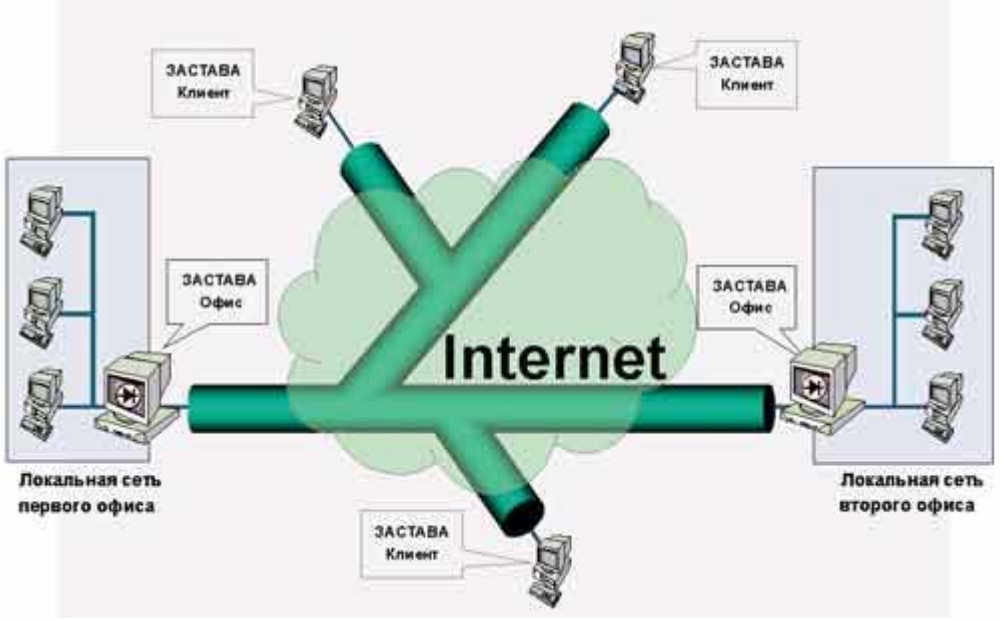
Надежная защита передаваемой по любым сетям информации возможна только криптографическими методами (шифрованием). Однако широко используемые системы защиты информации на уровне шифрования файлов, электронной почты и отдельных приложений уже перестают удовлетворять информационные службы банков. Растущие потребности банковского бизнеса требуют систем защиты, способных "на лету" защитить каналы между любыми клиент-серверными и интранет-приложениями, изолировать он-лайновые платежные системы, обеспечить защищенную связь с внешними клиентами банка.

Эти и многие другие задачи успешно решаются с помощью технологии виртуальных защищенных сетей (VPN - Virtual Private Networks). На рынке существует множество VPN систем, отличающихся подходами к организации защиты, используемыми стандартами. При выборе такой системы необходимо обратить внимание на изложенные ниже аспекты, описывающие основные характеристики VPN систем и решаемые ими задачи.

Прозрачность для приложений и пользователей. Используемый в большинстве VPN стандарт IPsec предполагает прозрачную шифрацию потока информации "на выходе" из компьютера. При правильной реализации стандарта IPsec приложения и пользователи банка продолжат обычную работу в сети, не замечая, что передаваемая/получаемая информация проходит этап шифрации/дешифрации. В этом случае создание VPN в вашем банке не останавливает производственный процесс, не вносит изменений в используемые прикладные системы и не требует обучения пользователей.

Решаемые задачи. Можно рассматривать VPN как защищенную броней информационную трубу между двумя или более компьютерами, участвующими в информационном обмене. Эти "трубы" затем могут прокладываться через потенциально опасные сети. VPN способна эффективно решать две задачи - защита внешних каналов и защита внутренних сетей.
Внешняя задача. На практике задача организации защищенного канала связи между несколькими офисами банка зачастую решается путем создания собственных выделенных каналов. Но даже столь дорогое решение не выдерживает никакой критики - ведь эти каналы проходят по неконтролируемой банком территории, через оборудование **разных провайдеров[1].** Используя зачастую основной протокол Internet - TCP/IP - и общее с Internet пространство адресов, в большинстве случаев такие каналы являются просто частью Internet, со всеми вытекающими отсюда опасностями.
VPN решает проблему контроля на всей протяженности канала. Более того, отпадает необходимость в собственных каналах. Например, можно подключить в каждом городе локальные сети филиалов банка к местному провайдеру Internet. Затем вы устанавливаете на пограничном с Internet компьютере каждого филиала программное обеспечение, выполняющее шифрование проходящей информации. Задача решена. Важно, чтобы VPN позволяла установить соответствующее программное обеспечение на отдельные компьютеры сотрудников, имеющих право доступа к вашим локальным сетям из дома или из гостиничного номера в командировке. Получившаяся картинка, где за основу VPN взяты продукты ЗАСТАВА компании ЭЛВИС+, представлена на рисунке:

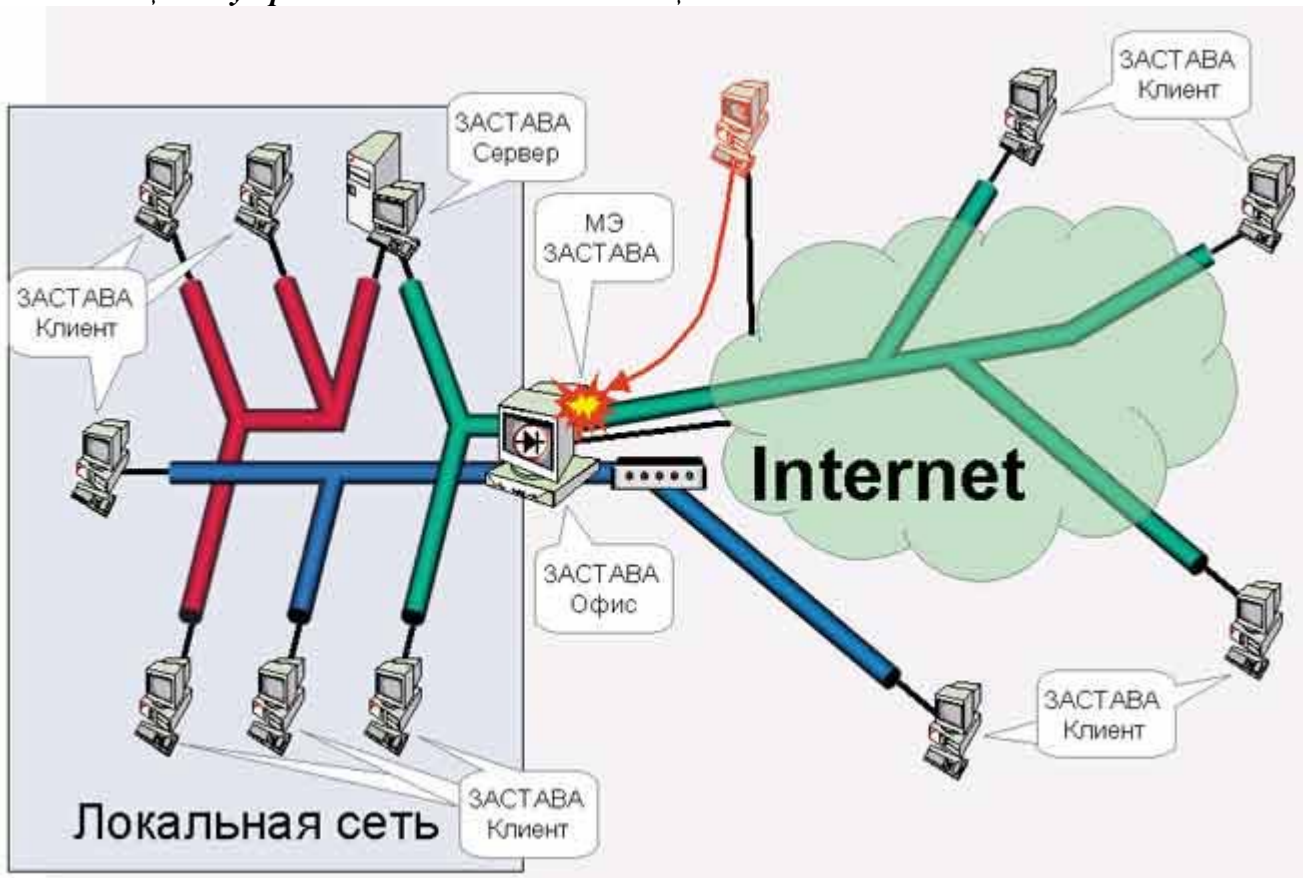
VPN позволяет проложить защищенные "трубы" через открытые сети и Internet



Таким образом, вы получаете свою собственную защищенную сеть (VPN), образующую жесткий непроницаемый периметр и наложенную на доступный всем Internet или любые другие сети. В локальную сеть каждого филиала смогут войти только защищенные и **аутентифицированные[2]** пакеты от других участников VPN. Эти пакеты, будут дешифроваться на выходе из "труб" и подаваться вышестоящим приложениям в первозданном виде.
Необходимо отметить, что технология VPN является не только способом защиты информации на внешних сетях. С потребительской точки зрения - это средство для создания ***дешевых, но надежно защищенных*** каналов через открытые сети и Internet.
Внутренняя задача. Присущий VPN эффект "защищенных труб" многие организации с успехом применяют и **на внутренних сетях[3].** Используемые сейчас локальные сети Ethernet работают по принципу "широковещания", посылая информацию по всем компьютерам сети, даже если она предназначена только для компьютеров кредитного отдела. VPN позволяет разделить информационные потоки различных подразделений банка. При этом новая сегментация будет

отражать только структуру бизнес-процессов и не будет зависеть от конкретной топологии внутренних локальных сетей.

Сегментация внутренних сетей банка с помощью VPN



На рисунке показана возможная схема реализации такого подхода. С помощью VPN ЗАСТАВА созданы три логически разделенные виртуальные сети (VPN).
Первая VPN (выделена красным цетом) включает 4 компьютера и находится целиком в локальной сети предприятия. Это VPN кредитного отдела. Вторая (выделена зелёным цветом) частично выходит во внешние сети, обеспечивая доступ к экстранет-серверу оператору из локальной сети и трем клиентам банка, подключенным через Internet. Третья VPN (выделена синим цветом) обеспечивает директору защищенный доступ из дома к своему рабочему компьютеру и компьютеру секретаря через модемный вход сервера доступа.
Все пользователи перечисленных VPN могут быть уверены, что их конфиденциальная информация доступна строго заданному кругу участников взаимодействия независимо от их местонахождения - внутри или снаружи стен банка - и способа доступа к сети.
Необходимая степень защиты. Основной задачей VPN является шифрование трафика, надежность которого определяется двумя функциональными характеристиками.
Первая заключается в стойкости используемых алгоритмов. Наиболее надежная защита строится только на проверенных временем и специалистами алгоритмах, утвержденных в многочисленных международных, государственных и отраслевых стандартах. Исключительно опасно полагаться на системы, надежность которых базируется только на том, что их авторы никогда не раскрывают сути и кода своих алгоритмов. В современной криптографии вся секретная часть защиты спрятана не в знании кода алгоритма, а в наличии ключа - длинного случайного числа, поданного на "вход" алгоритма вместе с защищаемыми данными.
Вторая характеристика - длина ключа, на котором производится шифрование. Не вдаваясь в подробности отметим, что минимально разумной длиной ключа на данный момент считается 128 бит.
К сожалению, огромное количество зарубежных систем защиты предлагают шифрацию очень надежными алгоритмами (например DES - американским государственным стандартом) на

совершенно неприемлемой длине ключа - 40 или 56 бит, что позволит легко вскрывать вашу информацию. Надо отдать должное российским стандартам, осуществляющим надежную защиту данных на очень длинных ключах - это государственный стандарт ГОСТ 28147-89 (ключ 256 бит) и отраслевой стандарт газовой промышленности ВЕСТА (ключ 512 бит). Вы можете смело доверять криптосистемам, работающим на этих алгоритмах.

Составляющие элементы системы. При всей своей простоте использования выбор VPN представляется достаточно сложной задачей. Надежная система, которая позволит вам на долгое время забыть о совместимости и болезнях роста сетей и задач, должна удовлетворять следующим требованиям:

- обязательная открытая поддержка стандарта защиты IPsec и одного из стандартов управления ключами (SKIP, ISAKMP или IKE) - гарантия надежности и работоспособности VPN независимо от ее размера;
- наличие полного ряда продуктов для защиты локальных сетей, серверных и клиентских платформ, что позволит строить схемы защиты, показанные на рисунках 1 и 2;
- возможность централизованного управления всей VPN;
- поддержка международного стандарта на **формат сертификатов[4]** X.509;
- поддержка **общепризнанных систем[5]** управления сертификатами (т.н. PKI, занимающихся **изготовлением, распределением и отменой[6]** сертификатов), что сэкономит вам в ближайшем будущем серьезные ресурсы, когда ваша VPN начнет расти в размере, распространяться на ваших партнеров/клиентов;
- поддержка **аутентификации пользователей[7]** VPN - способность VPN определить пользователя по его паролю, смарт-карте или ключевой дискете существенно защитит вашу систему "со стороны клавиатуры" (со стороны сети компьютер надежно закрыт самой VPN);
- открытость к другим системам защиты - одновременное хранение сертификатов разных систем на смарт-карте, обмен регистрационной информацией о работе пользователей и атаках между различными системами защиты.

Выбор поставщика VPN. В России существует целый ряд производителей различных VPN продуктов. В журнале "Сети и системы связи" N12 (46) от 1 октября 1999 г. ведущими специалистами ЦБ РФ была опубликована статья "Отечественные средства для построения виртуальных частных сетей", сравнивающая VPN продукты с технической точки зрения.

Среди этих продуктов выделяется полнотой функциональности и открытостью архитектуры масштабируемый ряд продуктов VPN ЗАСТАВА, появившийся на российском рынке в 1996 году. Многие территориально распределенные финансовые и промышленные компании внедрили VPN ЗАСТАВА в рамках опытной или промышленной эксплуатации: Банк России, Внешэкономбанк, Инкомбанк, Российский Кредит, Лукойл и другие. В настоящее время VPN ЗАСТАВА проходит тестирование в ряде российских и международных корпораций. VPN ЗАСТАВА применяется в этих организациях как для полной защиты трафика между филиалами, так и для сегментирования внутренних сетей.

VPN ЗАСТАВА отвечает практически всем описанным выше требованиям к VPN. Ее основные отличия - полный ряд продуктов для организации защиты сетей, серверов и клиентских компьютеров, а также поддержка всех основных международных стандартов - позволяют корпорациям и банкам рассчитывать на эффективную защиту сетей в любых конфигурациях и защиту своих инвестиций в будущем. VPN ЗАСТАВА включает в себя также систему распределенного FireWall, необходимость применения которого описана ниже.

Насколько опасно подключение к Internet?

Если вы подключились к Internet только для создания внутрибанковской VPN **(см.рис.1),** образующей жесткий периметр и не позволяющей никаких контактов с внешним миром, то Internet для вас не опасен. Он просто отключен от вас, вы используете его в транспортном режиме.

Ситуация усложняется, если вам все-таки необходимо общаться через Internet с внешним миром (получать сводки информационных агентств, участвовать в электронных торгах, обмениваться e-mail). В этом случае необходимо на границе VPN/Internet установить и использовать ряд достаточно хорошо отработанных технологий, как-то:
- системы FireWall на входе в сеть и на каждом из компьютеров сети - для защиты от прямых сетевых атак и проверки проходящей почты;
- системы антивирусного/антитроянского контроля на всех компьютерах пользователей;
- системы контроля и аудита за общей сетевой активностью, действиями пользователей и администраторов, атаками - т.н. intrusion detection;
- организационные технологии, связующие вместе всю систему безопасности.
Необходимо обеспечить также сочетание этих средств безопасности с уже существующими системами контроля доступа и информационной безопасности. К сожалению, объем статьи не позволяет более подробно остановиться на этой теме. Ее освещение планируется в одном из следующих номеров.
* * *
На современном рынке средств безопасности существует достаточное количество средств, способных не только надежно защитить ваши информационные ресурсы, но даже расширить возможности ваших информационных систем (как это происходит в случае использования VPN, до создания которых банки не могли использовать открытые сети для передачи конфиденциальной информации). С другой стороны, комплексность самого процесса создания многослойной и целостной защиты требует привлечения организаций, профессионально занимающихся системной интеграцией в области средств безопасности.

---

1 ***Провайдер*** *- организация, предоставляющая доступ к глобальным сетям передачи данных и/или Internet.*
2 ***Аутентифицировать*** *- гарантированно определить источник происхождения информации или ее автора.*
3 По данным ***ФБР*** *более половины* ***информационных атак*** *осуществляется* ***из внутренних сетей*** *организации.*
4 ***Криптографический сертификат*** *пользователя является аналогом паспорта пользователя. Это небольшой файл (около 800 букв), который пользователь хранит на своей смарт-карте или дискете. С его помощью он может шифровать и подписывать свои сообщения. Сертификат имеет срок жизни, определяемый при его создании.*
5 Например, ***PKI*** *компаний* ***Entrust, Verysign, Baltimor****e.*
6 ***Это одна из самых сложных задач для службы PKI****: как не позволить пользователю, чей сертификат отменен 2 часа назад, использовать этот сертификат для подключения к банковской VPN?*
7 Обычно ***VPN различает отдельные компьютеры****, но* ***может не отличить*** *стоящих за ними разных* ***пользователей****.*