Хакера обезвредят на "Заставе"
(информационная безопасность Internet-банкинга и Internet-трейдинга)

Евгений Ершов, руководитель направления по работе с финансовыми и фондовыми организациями компании "ЭЛВИС+"
Вестник НАУФОР №10, 2000 г.

В настоящее время мы наблюдаем ситуацию, когда Internet перерос рамки собственно информационной структуры и превратился в информационно-производственную структуру. Появление *Internet*-банкинга и *Internet*-трейдинга это наглядно подтвердило. Указанные технологии обладают к тому же активной динамикой расширения и практически неограниченным потенциалом развития. К сожалению, их широчайшие возможности открывают многообещающие перспективы и тем, кто не прочь погреть руки вблизи фондовых, финансовых и товарных потоков.

В период создания *Internet* никто не предполагал, что этот носитель информации нуждается в серьезной защите. "Беззащитность" невольно способствовала появлению в Сети сонма злоумышленников - от сетевых хулиганов до профессиональных сетевых преступников. В последнее время Запад захлестнула волна правонарушений в этой области. Подобная безотрадная перспектива ждет и Россию. Выявление факта преступления, его юридическое доказательство, адекватная оценка нанесенного ущерба и, особенно, его возмещение сталкиваются с большими трудностями и реализуются нечасто даже на высокоразвитом Западе.

Российские пользователи могут считать все это ближайшей собственной перспективой. Поэтому задачу защиты информационного обмена следует рассматривать в качестве первоочередной. Надо исключить возможность перлюстрации, модификации, фальсификации или иного использования элементов обмена злоумышленниками (деловой переписки, платежных документов, биржевых данных и другой критичной информации). Ситуация в России в настоящее время соответствует поговорке: "Не было бы счастья, да несчастье помогло". Информационные преступления пока не нанесли существенного ущерба российским бизнес-структурам из-за ее объективного отставания от Запада. Очевидно, что риск ущерба пропорционален не только объему и интенсивности информационного обмена, но ценности и критичности самой информации. Последствия опасностей, исходящих из *Internet*, едва ли не самые губительные для сфер финансового и фондового рынков. Они уступают лишь рискам, связанным с техногенными и военными катастрофами. Именно поэтому как никогда актуальна организация систем защиты информации (СЗИ), обеспечивающих бесперебойное и безопасное функционирование субъектов финансового и фондового рынков.

Специалисты фирмы "ЭЛВИС+" имеют опыт разработки средств и систем защиты информации для самых разных заказчиков: от крупных корпораций (в том числе с развитой филиальной сетью, насчитывающей сотни единиц вычислительной техники), до рядового брокера или бухгалтера, работающего на компьютере. Сформулируем ключевые моменты, характеризующие общие параметры таких средств и систем.

Политика информационной безопасности

Начальный этап - формулирование задач по защите информации. Исходя из состава и степени критичности информации, целей и способов ее обработки, определяются уровни и методы реализации защиты, а также состав организационно-технических мероприятий и базовых технических средств. Последнее хотелось бы подчеркнуть особо, поскольку, практика показывает, что опасность очень часто порождается отсутствием (равно как и несоблюдением) правил внутренней политики безопасности.

Предположим, на этапе разработки политики безопасности были учтены все необходимые организационно-технические требования. В результате вычислительные средства и средства связи (и, как следствие, информация) недоступны для лиц, специально не авторизованных к тому администрацией корпорации.
Следующий этап построения СЗИ - защита информации в процессе ее передачи по линиям связи между потребителями (биржевым терминалом и брокерами, рабочим местом бухгалтера и банковским сервером и т.п.).
Передача может осуществляться:

- по выделенным линиям связи;
- посредством открытых публичных коммуникационных сетей, прежде всего через Internet.

Первый путь не может рассматриваться как перспективный при увеличении информационного обмена "по горизонтали", например, расширении брокерской или филиальной сети. Это обусловлено, *во-первых*, тем, что приобретение специализированного оборудования, его установка и эксплуатация, а также аренда выделенных линий связи требуют солидных вложений денежных средств. Это не только единовременные расходы, но и регулярные платежи. Для большинства пользователей они весьма обременительны. *Во-вторых*, выделенные линии связи (даже будучи защищенными от электрических перегрузок, некорректной коммутации, неквалифицированного вмешательства и повреждения и т.п.) остаются незащищенными информационно.
Остается второй путь -*Internet*. Однако его использование сопряжено с серьезнейшим риском. Информационные ресурсы корпорации могут подвергнутся разного рода негативным воздействиям. Самые распространенные - атаки на информацию в процессе ее передачи между сегментами корпоративной сети. Поэтому вся критичная информация, передаваемая через *Internet*, должна быть надежно защищена.
Защита может осуществляться как аппаратными (например, встраиваемыми в компьютеры системами кодирования-декодирования данных), так и программными средствами (включением в программное обеспечение компьютеров специальных программных модулей кодирования-декодирования).
Первый способ, если его использовать для защиты сетей Internet-банкинга и Internet-трейдинга, страдает рядом недостатков. Один из самых существенных, (наряду с достаточно высокой стоимостью) - трудность изменения конфигурации защищаемых корпоративных и персональных сетей, добавления и (особенно) удаления пользователей таких сетей, изменения режима доступа различных пользователей к тем или иным информационным ресурсам. Подобная негибкая структура неприемлема для рассматриваемых *Internet*-приложений.
Более перспективен второй способ - программная защита информации, сочетающая высокую надежность, удобство наращивания функциональных возможностей и администрирования доступа пользователей информации к информационным ресурсам. Это позволяет создавать высоконадежные гибкие СЗИ, наиболее пригодные для *Internet*-банкинга и *Internet*-трейдинга.
Основная идея создания таких СЗИ - организация виртуальных частных сетей *(VPN - Virtual Personal Networks)*, т. е. системы своеобразных туннелей, проложенных внутри информационного пространства *Internet*. Их отличает возможность чисто программной реализации (без установки дополнительных специализированных аппаратных устройств)

и полная непрозрачность для внешнего наблюдателя (не только невозможность читать, модифицировать, повторять, удалять информацию, но и невозможность определить конфигурацию защищенных туннелями сетей, пользователей сетей и задач, решаемых этими пользователями).
Кроме того, технологии *VPN* позволяют путем удаленного администрирования менять конфигурацию "туннелированных" сетей, включая подключение и удаление пользователей, предоставление им доступа к информационным ресурсам (и отзыв этого доступа), а также множество других административных функций.
Эти возможности реализуются благодаря распространению среди пользователей как секретных, так и открытых ключей кодирования-декодирования информации. Технология реализуется программными средствами и не требует специальных средств доставки пользователям секретных ключей. По распоряжению руководства системный администратор биржи (банка) со своего рабочего места может предоставить брокеру (бухгалтеру, менеджеру) только санкционированный для него доступ к биржевым (финансовым, управленческим) информационным ресурсам.
Возможно обеспечение не только стационарного но и мобильного доступа пользователей к информационным ресурсам. Предлагаемые специалистами "ЭЛВИС+" технологии позволяют организовать защищенный доступ из любой точки мира, используя любой способ коммуникаций.
На рис.1 приведена эскизная схема, иллюстрирующая основные элементы сети для корпорации с двумя удаленными офисами, где элементами *VPN* являются продукты семейства "ЗАСТАВА".

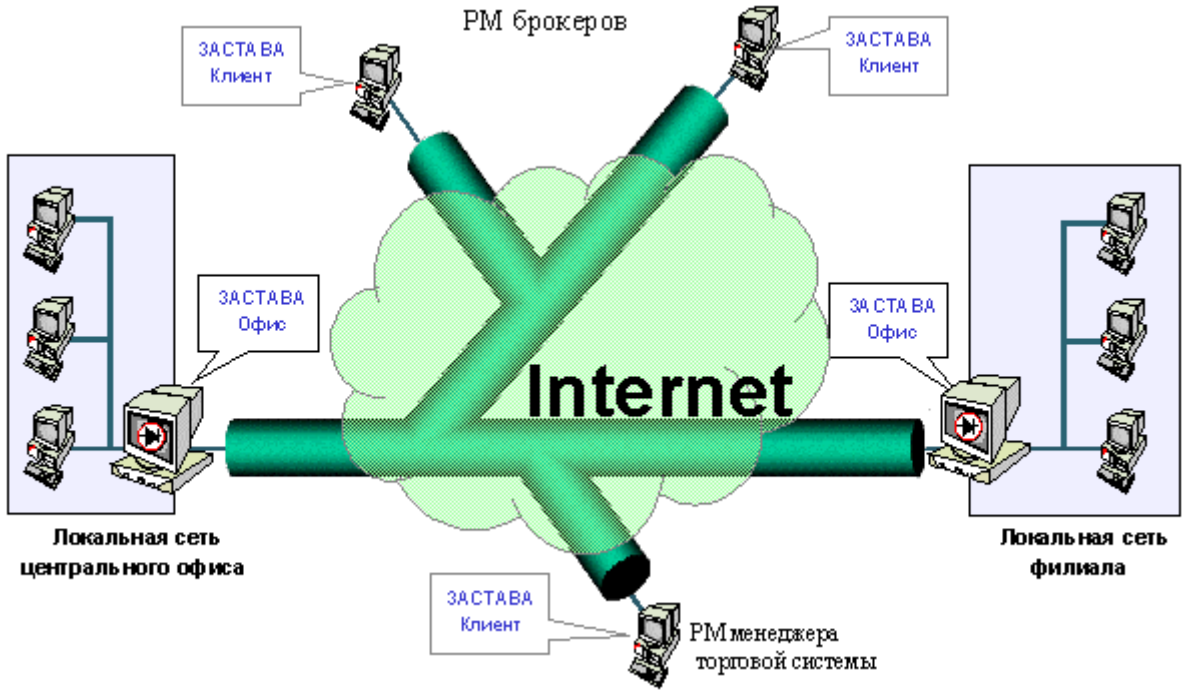

Рис. 1. Эскизная схема *VPN*.

Разумная открытость

В большинстве случаев полная изоляция внутренних информационных сетей банков и бирж (тем более, отдельных пользователей) от системы *Internet* неоправданна, как бы это ни выглядело заманчивым с точки зрения безопасности. Создание СЗИ предполагает разумную открытость по отношению к внешнему информационному пространству. При этом необходимо избегать ситуации, когда в хорошо защищенной внутренней сети банка

или биржи остаются незащищенные сегменты, обменивающиеся с внешним миром информацией в открытом виде. Они могут стать лазейкой для атак из внешней среды. Однако полностью избавляться от открытых сегментов нецелесообразно. Разумнее применять специальные программные продукты - межсетевые экраны, представляющие собой настраиваемые и управляемые фильтры, непрерывно обрабатывающие и анализирующие проходящий сквозь них информационный поток. Межсетевые экраны пропускают внутрь защищаемого сегмента сетей только безопасные информационные пакеты, отсеивая потенциально опасную, нежелательную и просто бесполезную информацию. Дополнительно рекомендуется включать в комплекс СЗИ специализированные программные модули - анализаторы уязвимости сетей, позволяющие отражать многочисленные виды сетевых атак (опасность которых, к сожалению, многими недооценивается), а также различные антивирусные средства.
На рис. 2 представлена схема более сложной организации сетей, на которой, помимо ранее изображавшихся элементов, присутствует межсетевой экран (МЭ) и программный продукт "ЗАСТАВА-Сервер".

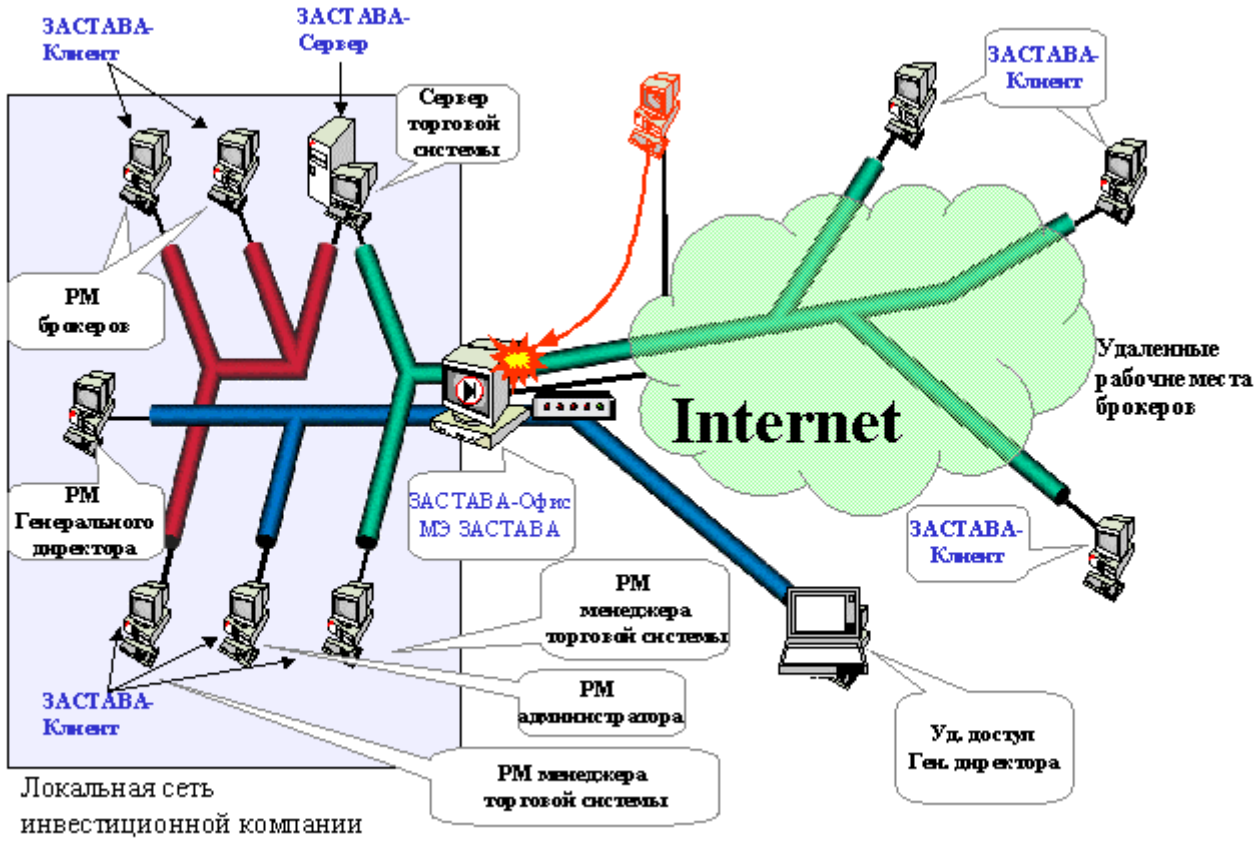

Рис. 2. Эскизная схема варианта реализации VPN

Масштабируемость решений и их непрерывность

На заре *Internet* никто не мог предположить какую роль он станет играть в жизни мирового сообщества, в том числе в экономической сфере. Сейчас трудно реально определить скорость количественного и качественного роста *Internet*-приложений. Однако, несомненно то, что этот рост будет быстрым. Поэтому при создании СЗИ надо предусматривать возможность их не только количественного, но и качественного наращивания с минимальными затратами ресурсов. Стало быть, одним из главных требований к корпоративной СЗИ должна стать ее масштабируемость.

Второе важное требование - непрерывность решений.
Этот пункт имеет две составляющих. *Первая* - **непрерывность программных продуктов:** применяемые решения должны быть совместимы с программными продуктами сторонних производителей. Полноценная СЗИ должна иметь такую структуру, которая без существенной перенастройки сможет функционировать со всеми программами, созданными на базе принятых международных стандартов на программные средства.
Вторая **- непрерывность во времени**. Разработчик СЗИ не только проектирует систему, но и постоянно ее модернизирует. Соответственно, СЗИ должна иметь постоянную поддержку разработчиков, обеспечивающую бесперебойное и корректное функционирование системы.
Таким образом *Internet*-банкинг и *Internet*-трейдинг объективно нуждаются в полноценных системах защиты информации. Такие системы должны проектироваться, разрабатываться, изготавливаться, устанавливаться и обслуживаться на основе полного, грамотного и корректного учета всех параметров и обстоятельств. Это подразумевает профессиональный подход на каждом этапе.
Компания "ЭЛВИС+", являясь системным интегратором, на основании выданных соответствующими государственными органами лицензий и сертификатов, на протяжении последних лет разработала и поставила ряд комплексных систем информационной безопасности по заказам компаний различного масштаба и назначения, в том числе фондового и банковского секторов экономики (например, АЛОР-ИНВЕСТ и Биржа "Санкт-Петербург") и показала себя способной эффективно и качественно работать на рынке современных информационных технологий.