Интернет-трейдинг и его Безопасность

И.Т. Кадощук "ЭЛВИС+", **С.А. Савельев** "ЭЛВИС+"
Рынок ценных бумаг №21, 2000 г.

Введение

Слова "электронная коммерция" или "е-бизнес" сегодня кажется популярнее, чем были "русские в космосе" в начале 60-х. Вместе с тем, по всеобщему мнению, электронная коммерция - явление далеко не новое и берет свое начало там же в 60-х. В течение всех этих лет бизнес пользовался системами электронного обмена данными (Electronic Data Interchange) для размещения заказов и их оплаты поставщикам. Однако, при этом, не использовались сети общего доступа. Их просто не было!
Что же сегодня имеют в виду, когда говорят электронная коммерция, e-Commerce, iCommerce, и пр.? Эксперты определяют электронную коммерцию, как торговлю товарами и услугами в которой окончательный заказ размещается через Inetrnet. Другими словами, электронная коммерция - это заключение сделок в электронной форме, а Интернет-торговля - только оплата покупок через Интернет, то есть, все таки, незначительная часть электронной коммерции. Сюда же относится и понятие Интернет-трейдинг (ИТр)- ведение через Интернет операций на фондовом рынке. Таким образом, хотя электронную коммерцию часто путают с Интернет-торговлей и Интернет-трейдингом, электронная коммерция более общее понятие.
Что содержит Интернет-трейдинг? Основными моделями ИТр являются открытие и ведение счетов, выставление и исполнение заявок на покупку или продажу ценных бумаг, получение информации о котировках, новостей, данных о финансовых показателях.
Откуда такая популярность? Это ведь не космос, а вполне заурядный процесс обмена коммерческой информацией, реквизитами и некоторыми подтверждениями. Неужели причиной является заурядная человеческая лень (пресловутый двигатель прогресса), и человечество просто не имеет времени на "непосредственное общение человека с человеком"? Впрочем, перспективы этого рынка впечатляют:

- По разным оценкам, емкость активной части рынка в 2000 году составит - от 5 до 20 тысяч отечественных инвесторов.
- Общий же объем мирового оборота электронной коммерции через Интернет в 2003 году предсказывают (Forrester Tech.) между $1.8 триллиона и $3.2 триллиона. Верхняя граница этой оценки достигается за счет всеобщего стремления сделать процесс покупки и продажи через Интернет простым, безопасным и повсеместно доступным. Медленное признание со стороны бизнеса и непримиримость со стороны государств и правительств могут серьезно препятствовать развитию электронной коммерции. В этом случае, мировой оборот достигнет только нижней оценки.

Таким образом, все-таки двигателем является извечное стремление человечества делать дорогое - дешевым, сложное - простым, недоступное - всеобщим и, желательно, "не вставая с дивана", или, другими словами, человеческая лень и скупость.
Однако обратим внимание на то, что же нам мешает? И здесь ключевыми словами будут: "безопасность", "медленное признание со стороны бизнеса" и "непримиримость со стороны государств и правительств". Попробуем разобраться, чего же опасаются правительства, бизнес и покупатель, что их беспокоит, в чем их неуверенность, и в чем их надежды? На первый взгляд, все как всегда: правительствам нужны налоги (т.е., точные данные кто сколько продал и купил), покупатели боятся пропажи денег (т.е. точные

данные, куда пошли деньги) случайной, а тем более, преднамеренной, бизнесам нужны покупатели (т.е. точные данные, где они находятся и что они предпочитают), и они также опасаются краж, т.к. бизнесы, как правило, являются и продавцами, и покупателями одновременно.
Таким образом, всем нужны точные данные по самым разным поводам, а значит, нужны эффективные механизмы их получения, безопасного хранения и обмена. Или, другими словами, большинство проблем бизнеса сегодня лежат в области информационной безопасности.
Так или иначе, но именно проблемы безопасности являются самым серьезным препятствием на пути бизнеса в Интернет!

Поставщики систем Интернет-трейдинга

Интернет-трейдинг объединяет множество различных функций. В простейшем виде, цель создания систем ИТр состоит в изменении способов ведения бизнеса при помощи новых технологий. Это может быть настолько же просто, насколько просто установить информационную связь между биржей и клиентом. ИТр использует новые технологии для изменения способов организации контакта покупателей и продавцов, методов представления, обсуждения и изменения заказа, операций и услуг, а также процесса осуществления платежей.
Сегодня многие компании, вдохновленные радужными перспективами электронной коммерцией вообще и ИТр в частности, предлагают разнообразное программное и техническое обеспечение. В частности, вот наиболее успешные из этих компаний в прошлом 1999 году (по данным наиболее авторитетного мирового рейтингового агентства FORBES):

Компания	**Оборот** (млн. USD)	**Год основания**
Поставщики программного обеспечения и услуг		
Microsoft	19,747	1975
Oracle	9,063	1977
Intuit	848	1983
Network Associates	785	1992
Cambridge Tech. Partners	628	1991
TMP Worldwide	585	1967
USWeb/CKS	375	1995
Citrix Systems	323	1989
Macromedia	167	1992

Network Solutions	142	1979
Concentric Network	110	1991
Exodus Communications	108	1992
BroadVision	71	1993
Inktomi	71	1996
Security First Technologies	44	1995
Razorfish	36	1995
Поставщики технического обеспечения		
IBM	87,448	1911
Lucent Technologies	38,303	1995
Intel	28,194	1968
Dell Computer	21,670	1984
Cisco Systems	12,154	1984
Sun Microsystems	11,726	1982
EMC	4,459	1979
Qualcomm	3,937	1981
Network Appliance	335	1992
Broadcom	335	1991
Juniper Networks	31	1992

И это действительно замечательный бизнес! Тут, кажется, есть повод, и для популярности, и для ажиотажа. В конце концов, если объем электронной коммерции достигнет такой громадной величины, как почти 10 % мирового торгового оборота в 2004 г., то эти, пусть и электронные, магазины, фондовые рынки и т.д. должен кто-то построить! И поставщики инфраструктуры стараются изо всех сил, создавая всевозможные необходимые компоненты!

Беззащитность Интернет-трейдинга

В целом поставщики программного обеспечения осознают проблему безопасности и, декларируя "абсолютную безопасность" использования собственных программных средств, встраивают в состав своих комплексов некоторые механизмы защиты, например, обеспечивающие идентификацию, туннелирование и шифрование конфиденциальных данных. Не смотря на это, мы постоянно слышим о взломах торговых систем и электронных магазинов, о краже таких достаточно конфиденциальных данных, как номера кредитных карт, причем кражах массовых - речь обычно идет о тысячах и десятках тысяч номеров, если не больше! И это только данные, попадающие в открытые средства информации.
Вместе с тем, по данным ФБР США ("Computer Crime and Security Survey"), в 1999 году потери частных и государственных структур США от вторжений в их информационные сети составили 265 млн. долларов (при среднем показателе в 120 млн. в течение трех предыдущих лет). Причем нападения различного рода были отмечены в 90%(!) отзывов от более чем 600 организаций и специалистов по компьютерной безопасности, которые приняли участие в опросе. В тоже время, 51% респондентов не смогли оценить собственные финансовые потери и только 31% респондентов смогли предоставить соответствующие данные. И это только зарегистрированный цифры! Многие попросту предпочитают молчать чтобы "не ударить в грязь лицом"!
Согласно специального доклада Белого Дома 2000 г., подготовленного администрацией президента США "National Plan for Information Systems Protection. Version 1.0", более 72 % компаний, фирм, корпораций, государственных и общественных организаций США обнаружили рост угроз безопасности их данных в течение последних двух лет. Основными причинами финансовых потерь, связанных с недостаточной информационной безопасностью являлись: компьютерные вирусы (76%), атаки изнутри (62%), атаки извне (25%), ошибки невнимательности (70%) и промышленный шпионаж (10%). Вот еще краткая подборка статистики по данным Института Компьютерной Безопасности ФБР США:

Типы нарушения систем информационной безопасности	% зафиксированных инцидентов	% приведших к потерям
Внешний несанкционированный доступ к корпоративной сети	**44%**	**25%**
Отказ в обслуживании	**32%**	**28%**
Подмена данных при передаче	**17%**	**18%**
Активное прослушивание	**2%**	**1%**
Внутренний несанкционированный доступ к сети	**97%**	**62%**
Внутренний несанкционированный доступ к информации	**55%**	**32%**

Для того, чтобы разобраться в необходимости и достаточности встраиваемых поставщиками механизмов информационной безопасности в специализированное программное обеспечение ИТр, следует более подробно рассмотреть весь спектр задач информационной безопасности.

Потенциальные опасности Интернет-трейдинга

В процессе функционирования систем ИТр потенциально возникает значительное число опасностей, например:

- Ответственность за безопасность при использовании сетей общего доступа, Интернет как правило перекладывается на пользователя. Интернет не принадлежит никому, никто не несет ответственности за управление, администрирование и безопасность в целом.
- Каналы доступа в Интернет могут дать возможность доступа к информационным ресурсам торговой организации извне.
- Неосторожное использование коммуникативных программ, в том числе, на основе HTTP-протокола, может привести к проникновению "троянских коней" - специальных программ-вирусов, нарушающих работоспособность и/или искажающих данные вашей информационной системы.
- Сети общего доступа часто используются специфически квалифицированными специалистами для проникновения незамеченными в системы безопасности информационных систем.
- Частое использование электронной почты может помочь злоумышленникам скомпрометировать имена пользователей торгующей организации. Специальные широко доступные в Сети программы могут быть использованы для поиска слабых мест в системах хранения пользовательских данных (имена, пароли, PIN-коды, и пр.) информационной системы.
- Интернет дает возможность пересылать конфиденциальную информацию практически в любую точку мира, однако, при этом, она может быть перехвачена, скопирована, искажена, прочитана, если недостаточно защищена, любыми внешними пользователями - злоумышленниками, конкурентами, любопытствующими, спецслужбами и пр.
- В частности, пересылая недостаточно защищенное платежное поручение, либо номера кредитных карточек, необходимо помнить, что пересылка идет не через частную/собственную сеть, и существует значительное число внешних пользователей имеющих потенциальную возможность манипулировать вашим сообщением; кроме вышеперечисленного, ваше сообщение может быть подменено: существуют методы отправки сообщений пользователем **A** так, как будто бы оно отправлено пользователем **B**.
- Сети общего пользования предоставляют много ценных служб их пользователям. Многие люди полагаются на эти службы в своей работе, так как они позволяют им эффективно решать свои задачи. Когда эти службы недоступны в нужный момент, производительность падает. Сеть может стать неработоспособной из-за специального пакета, чрезмерного количества вполне легальных пакетов, искажений при передаче или неисправного компонента сети. Вирус может снизить производительность или остановить систему ИТр. Подобного рода случаи называют "отказом в обслуживании" и представляют очень серьезную угрозу для ИТр.
- Интернет предоставляет доступ к ресурсам и услугам, которые могут делать труд персонала организации менее производительным, если внешняя активность персонала соответствующим образом не отслеживается и не корректируется.
- Защита информационных потоков организации защищена настолько, насколько является защищенным самое слабое место в информационной системе.

Безопасность обеспечивается целым набором методов и средств, и является одним из важнейших элементов систем ИТр. ИТр фактически невозможен без должной защиты. Объем потенциальных продаж в этой области электронной коммерции ограничивается страхом, который испытывают покупатели, продавцы и финансовые институты, обеспокоенные вопросами безопасности в Интернет. Этот страх основан в частности, на следующем:

- Отсутствие гарантии конфиденциальности - того, что кто-то может перехватить передачу ваших данных и попытаться найти ценную информацию, (например, номер вашей кредитной карточки, дату проведения операции, имя, адрес и т.д.)
- Недостаточный уровень проверки участников операции - без проверки участников транзакции одна из сторон может устроить маскарад, который может привести к оплате несуществующей сделки, когда деньги поступают не в фондовый магазин а вашему соседу по этажу. Например:
- Покупатель, посещая сайт, не уверен, что представленная на нем компания именно та за кого она себя выдает или он может передать номер своей кредиткой карточки (при использовании кредитных карточек, как средств платежа) лицу, которое не обладает достаточным уровнем полномочий.
- У продавца нет возможности проверить, что покупатель, сделавший заказ, является законным обладателем кредитной карточки.
- Наконец, нет гарантии целостности данных - даже если отправитель данных может быть идентифицирован, то возможно третья сторона изменит данные во время их передачи. Следовательно, необходим способ предотвращения вмешательства или метод определения модификации данных.

Еще одна проблема возникает как результат того, что многие компании занимаются разработкой программного обеспечения именно для ИТр. Это означает, что все участники фондовых операций должны иметь одни и те же приложения, что практически неосуществимо. Следовательно, необходим способ обеспечения механизма взаимодействия между приложениями различных разработчиков и интегрированного механизма управления.
Главным принципом ИТр и бизнеса любого типа является **интегрируемость и контактность -** бизнес процессов, информации и людей! Это, в частности, предполагает принципиальную открытость к интеграции, совместимости и интероперабельности к значительному спектру разнообразных программных средств самого различного назначения и локализации: от операционных систем, до библиотек графических интерфейсов пользователей, огромного количества и разнообразия поставщиков.
Такая интегрируемость в принципе невозможна без следования общественно согласованным **стандартам** и функциональным спецификациям самого высокого уровня! В том числе, и, если угодно, в первую очередь в области информационной безопасности!
Задачи информационной безопасности Интернет
Для поиска решений этих проблем был создан независимый консорциум - Inetrnet Security Task Force (ISTF) - общественная организация, состоящая из представителей и экспертов компаний-поставщиков средств информационной безопасности, электронных бизнесов и провайдеров Интернет инфраструктуры. Среди членов консорциума - лидеры рынка поставщиков электронной инфраструктуры, такие компании как Cisco Systems, eToys Inc., Sabre Inc., Travelocity, Verio Inc, и CA. Консорциум был создан специально для разработки технических, организационных и операционных руководств по безопасности Интернет нацеленных на предотвращение атак хакеров - террористов киберпространства.
Консорциум ISTF выделяет двенадцать областей информационной безопасности, на которых в первую очередь должны сконцентрировать свое внимание создатели

электронного бизнеса для того, чтобы обеспечить его работоспособность. Список, в частности, включает:

- Аутентификация (механизм объективного подтверждения идентифицирующей информации)
- Право на частную, персональную информацию
- Определение событий безопасности
- Защита корпоративного периметра
- Определение атак
- Контроль за потенциально опасным содержимым
- Контроль доступа
- Администрирование
- Реакция на события

Рекомендации ISTF предназначены для существующих или вновь образуемых систем ИТр. Рекомендации помогают определить потенциальные бреши и дыры в подобных компьютерных сетях, которые, если не обратить на них должного внимания, могут использоваться взломщиками-хакерами. Это может привести к атакам на систему ИТр, потрясениям и, даже, потенциальному крушению электронного бизнеса! Консорциум ISTF настоятельно рекомендует воспользоваться их наработками еще до организации электронной коммерции и бизнеса.
Начальный набор рекомендаций включает обстоятельства часто незаметные, но легко обнаруживаемые в большинстве систем, развертываемых сегодня в Internet. Они включают, в частности, требование не использовать значения, задаваемые "по умолчанию" во время установки и настройки приложений, т.к. это ведет к тому, что:

- установленные по умолчанию имена пользователей и пароли становятся широко известны;
- отсутствует защита от несанкционированного вторжения хакеров во внутреннюю и внешнюю сеть;
- отсутствует возможность организации аудита после проведения изменений в среде системы ИТр таких, например, как установка новых приложений и компьютеров;
- как правило, мы имеем дело с непрофессиональным и слабым администрированием, приводящем к неполному уничтожению устаревших имен пользователей и пр.

В случае с системами ИТр, информационная безопасность и защита являются критичными для непрерывности бизнеса как такового! Безопасность больше не является дополнительным свойством. Надежность системы 97% означает 293 потерянных для бизнеса часа в год!
Ценность ИТр и бизнеса создается **установлением контакта и интеграцией** бизнес процессов, информации и людей. Наиболее успешные электронные бизнесы существенно учитывают природу децентрализации Интернет. При изменении условий и появлении новых возможностей, новая функциональность должна быть доступна через web для любого сколь угодно удаленного пользователя. И если структура ИТр основана на **стандартах**, такой переворот может быть осуществлен за одну ночь - решающее преимущество в мире, где Быстрый съедает Большого!
Что является камнем преткновения информационной безопасности? Как не странно, некоторые краеугольные камни и принципы защиты ИТр, например, следующие:

-

- **Сложность приложений.** Логически "разгружая" клиентскую рабочую станцию, упрощая и унифицируя пользовательский интерфейс, мы все более усложняем приложения на сервере, а также процесс их разработки и окружающую среду эксплуатации. Интегрируя среду разработки и эксплуатации, мы можем радикально упростить разработку и эксплуатацию новых приложений.
-
- **Интеграция с существующими приложениями или другими системами.** Факт: статистически большая организация, фирма, корпорация поддерживает 6 операционных сред и более 150 различных приложений на рабочих станциях пользователей.
- Идеальное решение состоит в том, чтобы расположенные на сервере и/или клиентских станциях технологии в ИТр-системах были, как можно шире, основаны на **стандартах** и стандартных решениях! В этом мире можно гарантировать единственное: завтра все будет по-другому!

Возможности готовых решений

Для реализации основных функциональных компонент системы безопасности используют различные механизмы и методы:

- коммуникационные протоколы,
- средства криптографии,
- механизмы авторизации и аутентификации,
- средства контроля доступа к рабочим местам сети и из сетей общего пользования,
- антивирусные комплексы,
- программы обнаружения атак и аудита,
- средства централизованного управления контролем доступа пользователей, и безопасного обмена пакетами данных и сообщениями любых приложений по открытым IP-сетям.

Графически основные компоненты системы безопасности в ИТр выглядят, согласно классификации "рубежей обороны" *Hurwitz Group*, следующим образом:

Детальный анализ прикладных решений ИТр, поставляемых различными производителями показывает, что эти приложения реализуют только часть необходимых функций защиты и безопасности (не смотря на смелые декларации и всевозможные заверения, что те либо иные системы "абсолютно" безопасны и используют самые лучшие средства шифрования).
В этих системах, как правило, реализуют:

- функции защищенных коммуникаций с использованием специальных протоколов;
- функции контроля целостности данных, аутентификации и авторизации доступа пользователей в торговую систему;
- функции обеспечения конфиденциальности пересылаемых данных (реже).

Вместе с тем, ни одна из прикладных систем не может:

- контролировать целостность сети и всей информационной системы;
- защищать систему от неавторизованного вторжения из внутренней сети;
- защищать систему от неавторизованного вторжения из сетей общего пользования.

Как правило, прикладные решения ИТР:

- не интегрированы с системами контроля доступа пользователей к своим рабочим местам;
- ни одна из них не защищена от вирусов и от других типов "троянских коней".
- и, кроме того, процессы обнаружения несанкционированного доступа и аудита также реализуются внешними по отношению к торговой системе механизмами.

Наконец, можно сделать вывод, что ни одно из прикладных решений в области ИТр *не обеспечивает интегрированную комплексную управляемую систему информационной защиты* и подвержены значительным рискам потерь, искажений, компрометации информации и пр.

Согласно рекомендаций ISTF и классификации "рубежей обороны" *Hurwitz Group*, первым и важнейшим этапом разработки системы информационной безопасности электронной торговли и бизнеса будут механизмы управления доступом в и из сетей общего пользования, а также, механизмы безопасных коммуникаций, реализуемые межсетевыми экранами и продуктами частных защищенных виртуальных сетей (VPN). Сопровождая их средствами интеграции и управления всей ключевой информацией системы защиты - PKI - инфраструктура открытых ключей, мы получаем сравнительно целостную, централизованно управляемую систему информационной безопасности. Следующий рубеж включает в себя, интегрируемые в общую структуру, средства контроля доступа пользователей в систему вместе с системой однократного входа и авторизации (Single Sign On).
Антивирусная защита, средства аудита и обнаружения атак по существу завершит создание интегрированной целостной системы безопасности, если речь не идет о работе с конфиденциальными данными. В этом случае, потребуются также средства криптографической защиты данных и электронно-цифровой подписи.
Только некоторые их этих механизмов встраиваются поставщиками в готовые приложения ИТр и бизнеса. Остальную и главную работу по созданию информационной защиты и безопасности электронной коммерции и бизнеса должны делать именно специалисты по информационной безопасности - системные интеграторы в этой области. Без их участия ваша информационная защита всегда будет иметь потенциальные прорехи!