УДК 336

О НЕКОТОРЫХ ВОПРОСАХ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В БАНКОВСКОЙ СФЕРЕ

М.А. Романова[1], П.Д. Романов[2]
[1] УО "Полесский государственный университет", kazubomarina@yandex.ru
[2] Лицей УО "Полесский государственный университет"

Повышение информационной безопасности банка остается основным направлением развития информационных технологий в финансовой сфере. Этот фактор является определяющим при обеспечении надлежащей репутации банка, поскольку информационные системы вместе с преимуществами таят в себе и опасности, среди которых возможность несанкционированного доступа к информации и даже осуществления операций [1]. Особенно важен вопрос информационной безопасности в настоящее время, когда правительство Республики Беларусь планирует полный переход на электронный документооборот между всеми органами государственного управления и сведение к минимуму взаимодействие на бумажных носителях [2]. Информационная безопасность является важнейшим аспектом информационных технологий, так как направлена на защиту как клиентской, так и внутренней информации от несанкционированных действий. На сегодняшний момент это одно из немногих направлений автоматизации, бюджеты на которые не сокращаются, а даже увеличиваются в нынешних условиях [1].

Сети современных крупных банков нельзя назвать локальными в традиционном значении этого слова. Они состоят из множества подсетей и сегментов распределенных территориально и объединяемых различными каналами связи. Во многих случаях это означает, что банкоматы и обычные офисные компьютеры банков оказываются подключенными к одним и тем же вычислительным сетям. Как следствие, сети банкоматов, инфокиосков, обменных пунктов и др. могут быть подвержены всем существующим видам угроз — вирусным атакам, злонамеренным действиям персонала, ошибками администраторов и др.

В условиях, когда компьютерные системы становятся основой бизнеса, а базы данных — главным капиталом многих компаний, антивирусная защита прочно встает рядом с вопросами общей экономической безопасности организации. Особенно эта проблема актуальна для банков, по сути дела являющихся хранителями весьма конфиденциальной информации о клиентах, и бизнес которых построен на непрерывной обработке электронных данных [3].

Вследствие того, что вся информация в системах Интернет-банкинга между агентами передается по открытой сети, безопасности данных систем разработчики уделяют большое внимание. Для входа в саму систему клиенту, как правило, требуется ввести логин и пароль, что, в свою очередь, уже является определенным барьером для несанкционированного доступа. Естественно, необходимо защитить эту информацию от перехвата во время ее передачи от клиента к системе. Как правило, для этого используется такое стандартное средство, как протокол SSL (Secure Sockets Layer), который является обязательным атрибутом любого современного браузера. Протокол был разработан компанией Netscape в 1994 году. SSL обеспечивает шифрование всей передаваемой информации от компьютера клиента до сервера банка. Для повышения безопасности трансакций в Интернет-системах, как правило, предусмотрено использование клиентом электронно-цифровой подписи (ЭЦП). Именно по этой «подписи» система аутентифицирует пользователя и позволяет совершить необходимую операцию. ЭЦП – последовательность байтов,

формируемая путем преобразования подписываемого электронного документа специальным программным средством по криптографическому алгоритму и предназначенная для проверки авторства электронного документа. ЭЦП является подтверждением подлинности, целостности и авторства электронного документа. Обычно первоначальный обмен ключами между клиентом и банком осуществляется на внешних носителях без передачи ключей через открытые компьютерные сети. Секретный ключ клиента хранится на сервере сертификации банка и не имеет открытой публикации. На компьютер клиента для осуществления всех операций с ЭЦП устанавливается программное обеспечение, которое предоставляет банк. А все необходимые данные для клиента – открытый, закрытый ключ, идентификационные данные и пр. – обычно хранятся на отдельной дискете или в специальном аппаратном устройстве, которое подключается к компьютеру клиента [4].

С развитием интернет-банкинга банкам в той или иной мере приходится решать проблему безопасного подключения клиентов — ведь некоторые домашние компьютеры могут быть не защищены. Кража, уничтожение, искажение информации, сбой и отказ компьютерных систем — вот те проблемы, которые несут с собой вирусы и вирусоподобные программы [3].

Необходимо обеспечить безопасный доступ, с проверками удаленных рабочих станций, передаваемых протоколов, с гибкими возможностями централизованного управления. В частности, растет спрос на решения, обеспечивающие защиту web-трафика сотрудников: в последнее время резко увеличилось число проникновений вирусов в корпоративную сеть именно через web [5].

В связи с этим для обеспечения информационной безопасности различают многовендорный и моновендорный подходы.

С одной стороны, целесообразно использовать многовендорные решения, когда на различных уровнях корпоративной информационной системы устанавливается ПО различных производителей: на рабочих станциях, на почтовом сервере, на шлюзе выхода в интернет. Вирус, который не сможет отследить одна программа, будет блокирован другой, и наоборот.

С другой стороны, задачу обеспечения антивирусной защиты эффективнее решать на уровне защиты периметра сети, и производители ПО двигаются в этом направлении. Появляются комбинированные решения, которые помимо антивирусной защиты включают защиту от спама и систему фильтрации контента, т.е. отслеживания, что и куда отправляют пользователи. Комбинированные системы проще в администрировании, что приводит к значительному снижению совокупной стоимости владения [5].

Программно-технические компоненты системы антивирусной защиты должны обеспечивать формирование интегрированной вычислительной среды, удовлетворяющей следующим общим принципам создания автоматизированных систем:

- Надежность - система в целом должна обладать продолжать функционировать независимо от функционирования отдельных узлов системы и должна обладать средствами восстановления после отказа.
- Масштабируемость - система антивирусной защиты должна формироваться с учетом роста числа защищенных объектов.
- Открытость - система должна формироваться с учетом возможности пополнения и обновления ее функций и состава, без нарушения функционирования вычислительной среды в целом.
- Совместимость - поддержка антивирусным программным обеспечением максимально-возможного количества сетевых ресурсов. В структуре и функциональных особенностях компонент должны быть представлены средства взаимодействия с другими системами.
- Унифицированность (однородность) - компоненты должны представлять собой стандартные, промышленные системы и средства, имеющие широкую сферу применения и проверенные многократным использованием.

Как правило, защищают файл-сервера, сервера баз данных и сервера систем коллективной работы, поскольку именно они содержат наиболее важную информацию. Антивирус не является заменой средствам резервного копирования информации, однако без него можно столкнуться с ситуацией, когда резервные копии заражены, а вирус активизируется спустя полгода с момента заражения. Фактически, антивирусной защите подлежат все компоненты банковской информационной системы, связанные с транспортировкой информации и/или ее хранением:

- файл-серверы;
- рабочие станции;

- рабочие станции мобильных пользователей;
- сервера резервного копирования;
- сервера электронной почты.

Защита рабочих мест (в т.ч. мобильных пользователей) должна осуществляться антивирусными средствами и средствами сетевого экранирования рабочих станций. Средства сетевого экранирования призваны в первую очередь обеспечивать защиту мобильных пользователей при работе через Интернет, а также обеспечивать защиту рабочих станций ЛВС компании от внутренних нарушителей политики безопасности [6].

Белорусский рынок средств защиты в области информационной безопасности можно называть еще только формирующимся. Причем формирование это пока далеко от завершения.

На сегодняшний день на рынке Беларуси распространены программные средства защиты ряда компаний. Но многие из них, несмотря на требование законодательства, являются несертифицированными [7]. Продукты по обеспечению информационной безопасности на отечественном рынке представляют ЗАО ”БелХард Групп“, ГНПО ”Агат“, ЗАО ”АВЕСТ“, ЗАО ”НПП БЕЛСОФТ“, ООО ”Солидекс“, ”С-Терра Бел“, ООО ”Хедтекнолоджи Бел“, ОАО ”ЭНИГМА“, ”БелТим“ и др.

Таким образом, защита информационных систем от вирусов, шпионских программ и т.п. — важнейшая и постоянная задача общей системы экономической безопасности банка. Система защиты информации должна быть надежной, гибкой, должна постоянно совершенствоваться, чтобы выиграть время у лиц, пытающихся этой информацией завладеть. Следует ожидать, что будущее за комплексными системами информационной безопасности, что, в свою очередь, позволит оптимизировать величину бюджета информационной безопасности.

Список литературы:

1. Сацута Е.В. Итоги исследования банковских ИТ в 2011 году. [Электронный ресурс]. – Режим доступа: http://www.bankit.by/analytics/465-itogi-isled-banki-2011
2. Актуальные вопросы развития ИТ в банковской сфере были рассмотрены на ежегодном семинаре для руководителей служб автоматизации банков. [Электронный ресурс]. – Режим доступа: http://infopark.by/news/2013/4/29/art
3. Управление защитой информации — Лукашев В.М., Трубачев С.В.: Защита систем самообслуживания в банковских сетях. [Электронный ресурс]. – Режим доступа: http://belarus.iba.by/pub/uzi_10_1_2006.pdf
4. Ковалев, М.М. Информационные технологии в современном банке / М.М. Ковалев, С. Новик, К. Рихтер. //Вестник ассоциации белорусских банков. — 2004. — №13 (273). —С.54-61.
5. Аникеев А. Мультивендорная защита от вирусов. // [Электронный ресурс]. – Режим доступа: http://www.bosfera.ru/bo/2006/05/multivendornaya-zaschita-ot-virusov
6. Борисов В.И., Забулонов М.Ю. Организация системы антивирусной защиты банковских информационных систем. // [Электронный ресурс]. – Режим доступа: http://citforum.ru/security/virus/bank/
7. Попова Е.Э. Защита информации в компьютерных информационных системах и сетях. // [Электронный ресурс]. – Режим доступа: http://www.hist.bsu.by/images /stories/files/uch_materialy/dok/4_kurs/KITDOU_Popova/1.pdf