УДК 336.719

АНАЛИЗ СОВРЕМЕННОГО СОСТОЯНИЯ ЗАЩИТЫ БАНКОВСКОЙ ИНФОРМАЦИИ

Губенко Н.Е.[1)], Кибальченко А.В.[2)], Синяк А.А.[3)]
Донецкий национальный технический университет
[1)]к.т.н., доцент; [2,3)]студенты

Рассмотрены основные средства защиты информации, цели учета и контроль информации в банках. Определены способы защиты информации, а также наиболее часто используемые технологии информационной защиты. Проанализирована уязвимость информации в автоматизированных комплексах.

Мы живем в мире конкурентной борьбы за сферы влияния на международной арене, мировых рынках, за приоритеты в научной, военно-технической и экономической отраслях. Именно поэтому защита информации является неотъемлемой составляющей национальной безопасности.

В наше время информационные технологии (ИТ) занимают лидирующие позиции в развитии мирового сообщества и мировой экономики. Под информационными технологиями понимаются технологии обработки и управления даннями [1]. Главной целью должен являться процесс ускорения распространения информации при минимальных затратах. В наиболее развитых странах мира за счет информационных технологий стали появляться новые виды бизнеса, как например электронный. Он с легкостью удовлетворяет все возрастающие потребности общества, стирает границы между государствами и ускоряет развитие единого мирового рынка. В таких странах поддерживается инициатива внедрения ИТ для удовлетворения новых видов бизнеса, развития финансовых рынков, а также защиты потребителей информационной продукции и услуг.

К сожалению в нашей стране ИТ не развиваются на необходимом уровне. Общей целью является не оптимизация общего процесса, повышение производительности и, как следствие, экономический рост, а сиюминутная выгода, личные потребности. По мнению автора, Украине необходимо уменьшить госконтроль для создания конкурентоспособной бизнес-среды, что откроет для нее новые границы на международном рынке.

Одной из важнейших проблем функционирования банка, как такового, является проблема его безопасности, а точнее безопасности его информации. Защита банковской информации становится все более актуальной, выдвинувшись на первое место относительно физической охраны и средств технической защиты помещения банков.

За счет быстрого прогресса информационных технологий, финансовые учреждения начали внедрять открытые системы связи с выходом в Интернет, что привело к появлению новых каналов утечки информации и воздействия на нее. Таким образом, главными задачами защиты информации являются: обеспечение ограниченного доступа к конфиденциальной информации, защиты технических средств, обрабатывающих ее и безопасность передачи по каналам связи.

Данные о клиентах банков, их счетах и операциях интересны не только конкурентам, но и преступникам, которые для несанкционированного доступа к ним используют все возможные средства. Поэтому к банковским системам защиты конфиденциальной информации предъявляются особые требования.

Управление защитой – это контроль за распределением информации в открытых системах. Он осуществляется для обеспечения функционирования средств и механизмов защиты, фиксации выполняемых функций и состояний механизмов защиты, фиксации событий, связанных с нарушением защиты. Основные средства защиты – это шифрование данных при их хранении и при передаче по каналам связи, электронная цифровая подпись, а также средства защиты от несанкционированного доступа.

Учет и контроль в банке представлены операционным и бухгалтерским учетом, которые тесно связаны между собой, поскольку аналитический уровень отражен в банковском учете лицевыми счетами, а каждый лицевой счет находится под определенным балансовым. Основной целью аудита информационных систем является их контроль и анализ рисков, связанных с защищенностью, как от внешних, так и от внутренних факторов. Не существует возможности создать полностью защищенную систему. Даже при наличии неограниченного бюджета и ресурсов, всегда остается возможность того, что кто-то найдет путь для несанкционированного получения информации. Если совершенной безопасности невозможно достичь, то организация или банк должны определить

наиболее эффективный метод защиты информации, исходя из имеющихся ресурсов. По данным исследований CNews.ru наиболее востребованной технологией информационной защиты в банковской сфере являются системы аутентификации[2]. Это проверка принадлежности субъекту доступа к предъявленному им идентификатору, то есть, иными словами, проверка подлинности[1].

Способов аутентификации существует довольно много. Одним из наиболее часто используемых является текстовый ввод логина и пароля, но он далеко не единственный метод. Все большую популярность набирает аутентификация с помощью электронных сертификатов, пластиковых карт и биометрических устройств, например, сканеров радужной оболочки глаза или отпечатков пальцев или ладони.

В последнее время все чаще применяется так называемая расширенная или многофакторная аутентификация. Она построена на использовании нескольких компонент, таких, как: информация, которую пользователь знает (пароль), использовании физических компонентов (например, идентификационные брелки или смарт-карты), и технологии идентификации личности (биометрические данные).

Наиболее часто используемыми технологиями информационной защиты в банковской сфере являются антивирусы, комплексы кодирования межсетевых потоков, межсетевые экраны и защищенный WEB-сервер. Межсетевые экраны осуществляют контроль и фильтрацию проходящих через него сетевых пакетов на различных уровнях модели OSI, в соответствии с заданными правилами. Его основной задачей является защита компьютерных сетей или отдельных узлов от несанкционированного доступа. Также сетевые экраны часто называют фильтрами, так как их основная задача – не пропускать (фильтровать) пакеты, не подходящие под критерии, определенные в конфигурации.

Однако анализ существующего положения показывает, что уровень мероприятий по защите информации, как правило, отстает от темпов автоматизации. Одной из основных причин этого отставания является неразвитость и неотрегулированность рынка криптографической продукции.

При этом, недостаточно учитываются отличия банковской информации от традиционных объектов криптографической защиты (военные и государственные секреты), что приводит к завышенным требованиям к средствам криптографической защиты банковской информации.

Уязвимость информации в автоматизированных комплексах обуславливается большой концентрацией вычислительных ресурсов, их территориальной распределенностью, долговременным хранением больших объемов данных на магнитных носителях, одновременным доступом к ресурсам большого числа пользователей различных категорий. Автоматизированный комплекс можно считать защищенным, если все операции выполняются в соответствии со строго определенными правилами, которые обеспечивают непосредственную защиту объектов, ресурсов и операций. Основу для формирования требований к защите составляет список угроз. Когда такие требования известны, могут быть определены соответствующие правила обеспечения защиты. Эти правила, в свою очередь, определяют необходимые функции и средства защиты. Чем больше требований к защите и соответствующих правил, тем эффективнее механизмы защиты и тем более защищенным оказывается автоматизированный комплекс.

Исключительно важным элементом для платежной системы является защита юридической значимости платежных документов для справедливого разрешения споров и определения виновных в нанесенном ущербе, так как только юридическая защищенность создает доверие к системе платежей у ее участников и повышает их дисциплинированность при совершении расчетов. Это является еще одним аргументом в пользу того, что для платежной системы более приоритетными являются криптографические методы обеспечения подлинности и целостности платежных документов, а не методы обеспечения конфиденциальности.

Защита банковской информации при ее передаче по телеграфным и почтовым каналам связи осуществляется, в основном, организационными мерами, в сочетании с использованием криптографических средств – системы кодов подтверждения. В отдельных регионах, использующих для передачи информации модемную связь, в качестве средств защиты применяются средства шифрования и электронной цифровой подписи (ЭЦП) различных фирм-производителей криптопродуктов.

ЭЦП – реквизит электронного документа, предназначенный для защиты этого документа от модификации, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе[1]. Порядок применения цифровой подписи в банковской деятельности

определяется Национальным банком Украины. Обслуживание физических и юридических лиц совершается центром сертификации ключей на договорных основаниях.

К сожалению, у большинства средств криптографической защиты нет необходимых сертификатов, что приводит к несовершенной системе защиты и утере информации.

Специально для банковских систем в теоретической криптографии существуют два направления разрабатываемых исследований. Это криптографические протоколы и криптографическое обеспечение банковских карточек.

На рисунке 1 представлен график соотношения эффективности методов защиты банковской информации от их стоимости.

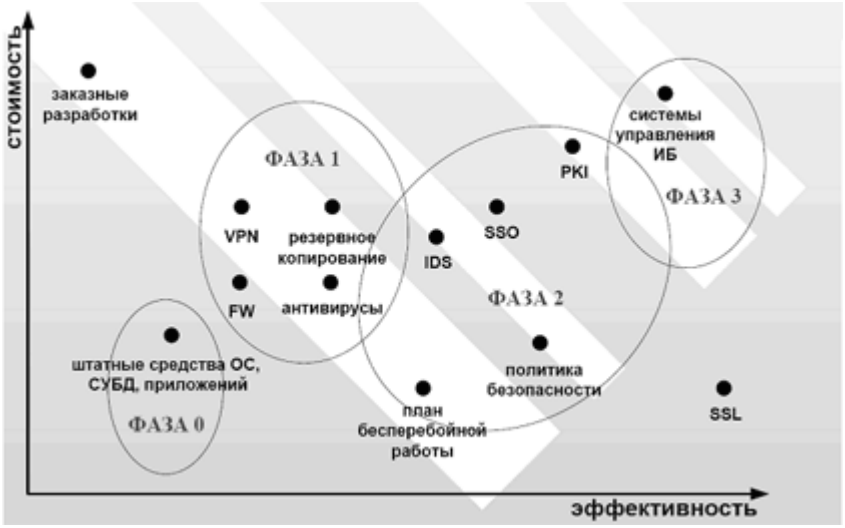

Рисунок 1 – Соотношение эффективности методов защиты банковской информации от их стоимости

На рисунке 2 изображены средства и методы защиты информации, которые составляют основу механизмов защиты.

Рисунок 2 – Методы и средства обеспечения безопасности информации

Рассмотрим основное содержание представленных методов и средств защиты информации.

Препятствие – метод физического преграждения пути злоумышленнику к защищаемой информации (к аппаратуре, носителям информации и т.д.).

Управление доступом – метод защиты информации регулированием использования всех ресурсов компьютерной информационной системы банковской деятельности (элементов баз данных, программных и технических средств). Управление доступом включает следующие функции защиты: идентификацию пользователей, персонала и ресурсов системы, их опознание (установление подлинности) по предъявленному им идентификатору, проверку полномочий, разрешение и создание условий работы в пределах установленного регламента, регистрацию обращений к защищаемым ресурсам, реагирование (сигнализация, отключение, задержка работ, отказ в запросе) при попытках несанкционированных действий.

Маскировка – метод защиты информации путем ее криптографического закрытия. Метод защиты широко применяется за рубежом для обработки ихранении информации. При передаче информации по каналам связи большой протяженности этот метод является единственно надежным.

Регламентация – метод защиты информации, создающий такие условия автоматизированной обработки, хранения и передачи защищаемой информации, при которых возможности несанкционированного доступа к ней сводились бы к минимуму.

Принуждение – такой метод защиты, при котором пользователи и персонал системы вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности.

Побуждение – такой метод защиты, который побуждает пользователя и персонал системы не разрушать установленные порядки за счет соблюдения сложившихся моральных и этических норм.

Рассмотренные методы обеспечения безопасности реализуются на практике за счет применения различных средств защиты, таких, как технические, программные, организационные, законодательные и морально-этические. К основным средствам защиты, используемым для создания механизма защиты, относятся следующие:

• Технические средства реализуются в виде электрических, электромеханических и электронных устройств. Вся совокупность технических средств делится на аппаратные и физические. Под аппаратными техническими средствами принято понимать устройства, встраиваемые непосредственно в вычислительную технику или устройства, которые сопрягаются с подобной аппаратурой по стандартному интерфейсу.

• Физические средства реализуются в виде автономных устройств и систем. Например, замки на дверях, где размещена аппаратура, решетки на окнах, электронно-механическое оборудование охранной сигнализации.

• Программные средства представляют из себя программное обеспечение, специально предназначенное для выполнения функций защиты информации.

• Организационные средства защиты представляют собой организационно-технические и организационно-правовые мероприятия, осуществляемые в процессе создания и эксплуатации вычислительной техники, аппаратуры телекоммуникаций для обеспечения защиты информации.

• Морально-этические средства защиты реализуются в виде всевозможных норм, которые сложились традиционно или складываются по мере распространения вычислительной техники и средств связи в обществе. Эти нормы не являются обязательными как законодательные меры, однако, несоблюдение их ведет обычно к потере авторитета и престижа человека.

• Законодательные средства защиты определяются законодательными актами страны, которыми регламентируются правила пользования, обработки и передачи информации ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил.

Все рассмотренные средства защиты разделены на формальные (выполняющие защитные функции строго по заранее предусмотренной процедуре без непосредственного участия человека) и неформальные (определяются целенаправленной деятельностью человека либо регламентируют эту деятельность).

Не смотря на то, что нынешние банковские системы используют огромное количество средств защиты, уровень защищенности информации не соответствует требованиям современных банковских информационных систем. Финансовые учреждения, использующие информационные технологии для развития бизнеса, должны осознать важность безопасности информации. Учитывая бурный прогресс технических новшеств, нельзя дать однозначных рекомендаций по информационной безопасности для каждого финансового учреждения. Можно ожидать, что в скором времени, банки возьмут под полный контроль состояние информационной безопасности в финансовых учреждениях и будут способствовать ее совершенствованию, включая проведение экспертиз с акцентом на безопасность информации.

Список использованных источников

1. http://ru.wikipedia.org/wiki/Информационные технологии.
2. http://www.cnews.ru/reviews-/free/finance/security/.
3. Анохин М. И. Криптография в банковском деле / М. И. Анохин, Н. П. Варновский, В. М. Сидельников, В. В. Ященко. – 1997. – 233 с.
4. Домарев В. В. Безопасность информационных технологий. Методология создания систем защиты / В. В. Домарев. – К. : ООО "ТИД "ДС", 2002. – 688 с.
5. http://www.prostobankir.com.ua/it/stati/informatsionnye_tehnologii_it_ne_roskosh-_a_put_k_pobede.
6. http://capri.ustu.ru/banking_systems/%C3%EB%E0%E2%E0%201.htm.
7. Титоренко Г. А. Информационные системы в экономике / Г. А. Титоренко. – М. : "ЮНИТИ-ДАНА", 2008. – 463 с.