УДК 003.26

АНАЛИЗ АТАК И МЕТОДОВ ЗАЩИТЫ ВО ВНУТРИПЛАТЕЖНЫХ БАНКОВСКИХ СИСТЕМАХ

Мороз М.О., студент; Сазанов М.Ф., студент;Губенко Н.Е., к.т.н., доц.
(Донецкий национальный технический университет, г.Донецк, Украина)

В развитии рыночных отношений главенствующую роль играют коммерческие банки, аккумулирующие огромные финансовые потоки. Информационные банковские системы становятся одной из наиболее уязвимых сторон современного банка, притягивающие к себе злоумышленников, как из числа персонала банка, так и со стороны.

Нарушение работы банковских систем приводит к потере не только конфиденциальной информации банка, но и к экономическому ущербу как банка, так и его клиентов, что создает общенациональную проблему.

Целью статьи является анализ угроз информационных данных во внутриплатежных банковских системах (ВПБС), рассмотрение уже существующих моделей пассивной и активной атак, исследование основных направлений защиты ВПБС.

Внутриплатежная банковская система представляет собой правила, организационные мероприятия, программно-технические средства, средства защиты, используемые банком для выполнения внутрибанковского и межбанковского перевода денег. Данная система относится к числу многоуровневых критических систем ,т. к. ее отказ, отступление от задаваемых ограничений либо изменения в работе подсистемы могут повлечь за собой серьезные последствия либо привести к краху всей системы в целом.[1]

Для обеспечения защиты банковской информации в ВПБС на различных уровнях используются криптографические механизмы, однако бурный рост вычислительной техники, приводит к появлению новых угроз (активных и пассивных атак) и взлому подсистемы защиты ВПБС. Под угрозой понимается совокупность условий факторов, создающих опасность несанкционированного, в том числе случайного, доступа к информации, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение информации.[2]

Подтверждением этому являются широко известные факты утечки информации: базы данных одного из крупнейших банков Великобритании – «Royal Bank of Scotland» в Атланте (9 млн. долл., 2009 г.); секретных документов и разработок Lockheed Martin (ущерб более 1 млрд.долл., 2006 г.);

Все источники угроз безопасности информации можно разделить на три основные группы: умышленные угрозы безопасности в ВПБС, стихийные бедствия и сбои.

Одним из наиболее уязвимых мест в системе электронных платежей является пересылка платежных и других сообщений между банками, между банком и банкоматом, между банком и клиентом.

Основным методом оценки возможностей злоумышленника при атаке есть создание модели атаки. Рассмотрим основные модели атак на ВПБС.

Пассивные модели угрозы вытекают из прослушивания и не связаны с каким-либо изменением информации. Суть атаки заключается в том, что при передаче криптограммы *El* в точку приема по некоторому каналу нарушитель выполняет мониторинг сети. При этом нарушитель (криптоаналитик) обязан владеть всеми открытыми параметрами и данными, которые используются субъектами *s*, выполняющими обмен данными. В таком случае криптоаналитик может провести криптоанализ протокола с целью определения сеансовых или долгосрочных ключей, которые используются субъектами – участниками протокола.[3]

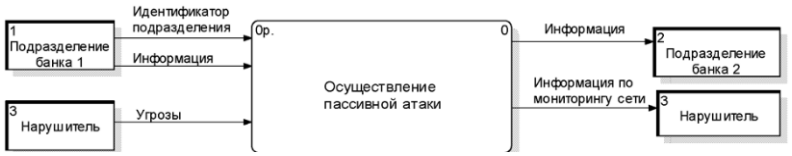

Рисунок 1 – Обобщенная модель пассивных атак

Таким образом, криптоанализ представляет собой решение математической задачи с целью определения самого сообщения или некоторых личных ключей субъектов – участников протокола. Более опасными с точки зрения экономического ущерба для ВПБС являются активные атаки.

Существует несколько типов активных атак: атака на ВБПС с блокировкой передачи информации; атака на ВБПС с внесеним помех; атака на ВБПС «Маскарад».

Суть атаки с блокировкой передачи информации заключается в том, что нарушитель, определив факт выполнения криптографического протокола, блокирует передачу информации, в результате чего криптограмма не достигает приемной стороны. Таким образом, при реализации данной атаки необходимые данные не достигают получателя, что приводит к потере конфиденциальной информации.

Суть атаки с внесением помех заключается в том, что нарушитель, определив факт выполнения криптографического протокола, вносит некоторую ошибку *e* и передает в точку приема криптограму (*El* + *e*). На приемном конце с помощью обратного отображения *i*–1 (заданного ключом) из криптограммы (*El* + *e*) восстанавливается недостоверная информація *Ije* = *i*–1(*Ki*, El* + *e*) ,т. е. подразделение банка получает сообщение, отличное от исходного *Ije* ≠ *Ij*. Реализация данной атаки приведет к получению на приемной стороне ложной транзакции.

Суть атаки «маскарад» заключается в том, что пользователь передает информацию от имени другого пользователя. Способы замены идентификатора могут быть разные, обычно они определяются ошибками и особенностями сетевых протоколов. Тем не менее, на приемном узле такое сообщение будет воспринято как корректное, что может привести к серьезным нарушениям работы ВПБС.

Для предотвращения угроз на информационные ресурсы ВПБС рассмотрим основные направления защиты банковской информации,показанные на рисунке 2.

Рисунок 2 – Основне направления защиты банковской информации

Анализ средств защиты показал, что большинство из них реализовано с помощью аппаратных, программно-аппаратных и программных систем и средств, на основе соответствующих криптографических алгоритмов. Достоинством аппаратных

средств является их простота реализации, недостатком – невозможность совершенствования и модернизации, возможность «обхода» злоумышленником .

Достоинством программно-аппаратных средств является функция стирания секретной информации при попытках физического проникновения в аппаратную часть системы, возможность модернизации и совершенствования используемых криптоалгоритмов, недостатком – высокая стоимость по сравнению с программными средствами защиты. Учитывая экономическую эффективность системы обеспечения безопасности, чаще применяют только программные средства. Программные средства предоставляют гибкую, обеспечивающую достаточный уровень защиты,и в то же время незначительную по стоимости обслуживания программных комплексов систему.[4]

На рисунке 3 приведена взаимосвязь основных направлений и средств защиты информационных ресурсов в ВПБС.

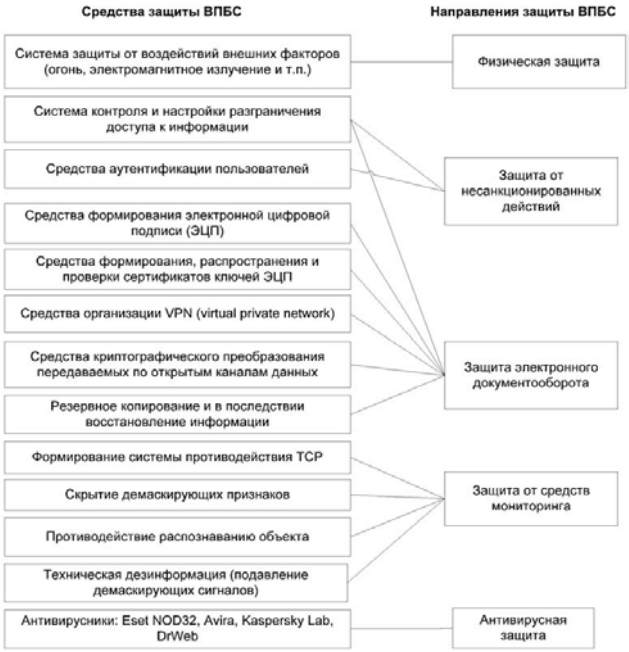

Рисунок 3 – Взаимосвязь основных направлений и средств защиты информационных ресурсов в ВПБС

Проведенный анализ показал, что для обеспечения надежной защиты необходим комплексный подход, включающий в себя анализ общей структуры ВПБС, возможных угроз и реализованных атак; выбор ратифицированных стандартов для обеспечения аутентичности, целостности и конфиденциальности банковских транзакций.

Перечень ссылок

1. Евсеев С. П. Построение атак на внутриплатежные банковские системы / Евсеев С. П. , Король О. Г., Гончарова А. И.Материалы из научной конференции «Радіоелектроніка, інформатика, управління. 2010. № 1.»
2. Глоссарий [электронный ресурс]. – Электрон. дан. Режим доступа: http://www.glossary.ru.
3. В. Столлингс. Криптография и защита сетей: принципы и практика : пер. с англ. – 2-е изд. – М. : Вильям. с.2001. – 672 с.
4. Кузнецов О. О. Захист інформації та економічна безпека підприємства : монография / О. О. Кузнецов, С. П. Євсеєв, С. В. Кавун. – Х. : ХНЕУ, 2008. – 360 с.