УДК 621.391

Евсеев С. П.[1], Король О. Г.[2], Гончарова А. И.[3]

[1]Канд. техн. наук, доцент Харьковского национального экономического университета

[2]Преподаватель Харьковского национального экономического университета

[3]Студент Харьковского национального экономического университета

ПОСТРОЕНИЕ МОДЕЛЕЙ АТАК НА ВНУТРИПЛАТЕЖНЫЕ БАНКОВСКИЕ СИСТЕМЫ

Анализируются угрозы информационных данных во внутриплатежных банковских системах (ВПБС). Разрабатываются модель реализации угроз информационных данных в ВПБС, математические модели пассивной и активной атак, исследуются основные направления защиты в ВПБС.

Ключевые слова: угрозы, внутриплатежная банковская система, математическая модель, модель реализации угроз, пассивная атака, активная атака, защита, шифрование, аутентичность, целостность.

ВВЕДЕНИЕ

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 [1–3].

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 в ВПБС, построение общей структуры подсистемы защиты информации, структурной схемы модели реализации угроз информационных ресурсов, математических моделей пассивной и активной атак, исследование основных направлений защиты во ВПБС.

1. Анализ угроз безопасности ВПБС. *Внутриплатежная банковская система* представляет собой совокупность правил, организационных мероприятий, программно-технических средств, средств защиты, используемых банком для выполнения внутрибанковского перевода денег, а также для взаимодействия с другими банковскими платежными системами для обеспечения выполнения межбанковского перевода денег филиалами банка [2]. 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.

Для обеспечения защиты банковской информации в ВПБС на различных уровнях используются криптографические механизмы, однако бурный рост вычислительной техники, создание систем и технологий кибертерроризма 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 [4]. Подтверждением этому являются широко известные факты утечки информации: данных из ядерной лаборатории Los Alamos (2007 г.); базы данных NASA о новых проектах (ущерб более 720 тыс. долл., 2006 г.); базы данных клиентов крупнейшего японского банка Mizuho (ущерб более 100 миллионов йен, 2006–2009 г.г.); базы данных одного из крупнейших банков Великобритании – «Ройял бэнк оф Скотлэнд» в Атланте (9 млн. долл., 2009 г.); секретных документов и разработок Lockheed Martin (ущерб более 1 млрд. долл., 2006 г.); Формулы-1: утечка данных из Феррари в МакЛарен (2008 г.) [1].

Все источники угроз безопасности информации можно разделить на три основные группы: умышленные угрозы безопасности в ВПБС, стихийные бедствия и сбои. На рис. 1 приведена общая классификация угроз информационных ресурсов в ВПБС.

Одним из наиболее уязвимых мест в системе электронных платежей является пересылка платежных

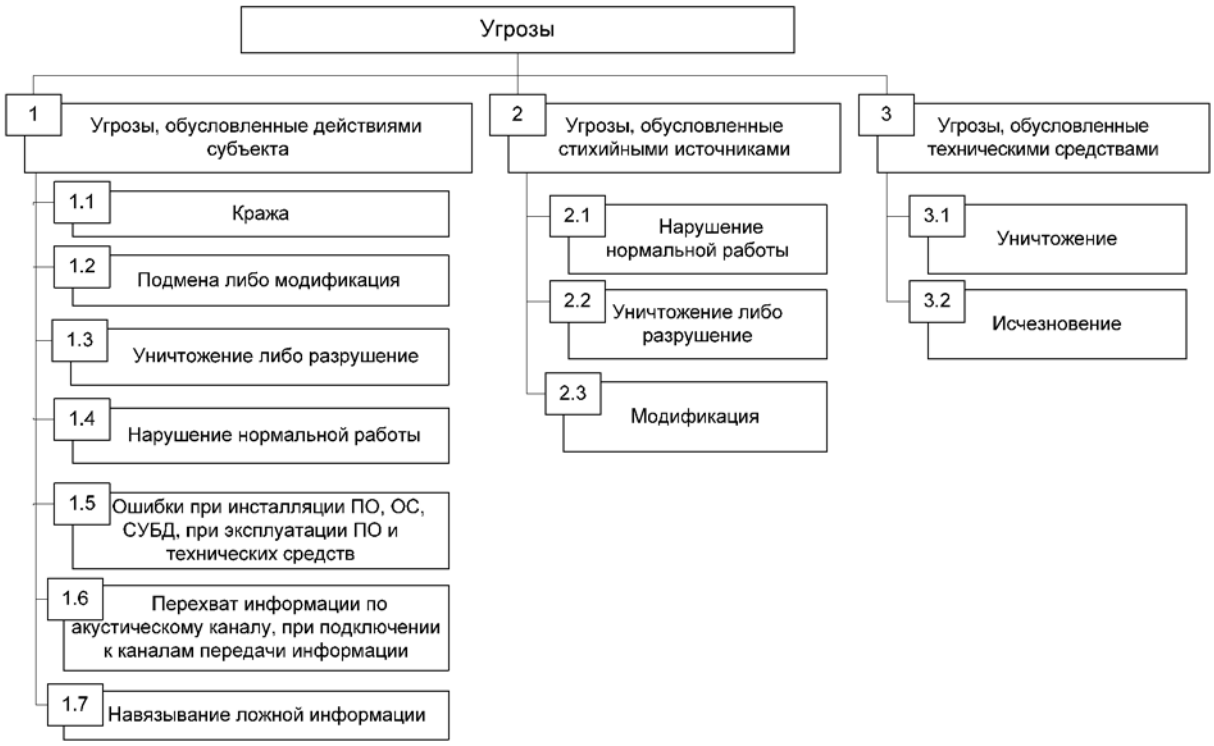

Рис. 1. Общая классификация угроз информационных ресурсов в ВПБС

и других сообщений между банками, между банком и банкоматом, между банком и клиентом.

Для защиты платежных сообщений используется система защищенной электронной почты (СЗЭП), предназначенная для обмена электронными сообщениями в формате SMF-70 через сеть передачи данных произвольного типа в соответствии с критериями НД ТЗІ 2.5-004-99 [3]. Общая структура подсистемы защиты информации в ВПБС и возможных угроз ее отдельным составляющим представлена на рис. 2.

Для совершенствования подсистемы защиты ВПБС в условиях появления новых угроз необходим постоянный анализ риска проведения той или иной атаки (реализации угрозы). Перечень угроз, оценка вероятности их реализации, а также модель нарушителя служат основой для проведения анализа риска и формулирования требований к системе защиты ВПБС. Таким образом, анализ угроз в конкретных условиях составляет основу для планирования и осуществления мероприятий, направленных на обеспечение безопасности ВПБС, в том числе: на формирование обоснованных требований по защите, методов оценки экономического ущерба, нанесенного вследствие реализации угрозы (проведения атаки) нарушителем, выбор конкретных механизмов, систем защиты информационных банковских ресурсов и транзакций. Однако в полной мере все это невозможно выполнить без построения и анализа модели реализации угроз и моделей пассивных и активных атак.

1. ПОСТРОЕНИЕ МОДЕЛИ РЕАЛИЗАЦИИ УГРОЗ БЕЗОПАСНОСТИ ВПБС

Моделирование процесса реализации угроз безопасности ВПБС целесообразно осуществлять на основе рассмотрения логической цепочки: «угрозы – источник угрозы – метод реализации – уязвимость – последствия». На рис. 3 представлена структурная схема модели реализации угроз информационных ресурсов в ВПБС.

Для описания модели реализации угроз информационных ресурсов в ВПБС (математических моделей активной и пассивных атак) зафиксируем конечное множество субъектов, взаимодействующих с информационной системой (S). Под *субъектом* s подразумеваем организацию, группу, одного человека или программно-аппаратное средство, способное принимать активное участие в процессе функционирования системы, то есть оказывать прямое влияние на нее. Определим рост атак на компьютеры субъекта S.

Пусть параметр N – количество уязвимых к атаке компьютеров (ПК), а параметр D содержит начальное значение среднего количества атакованных

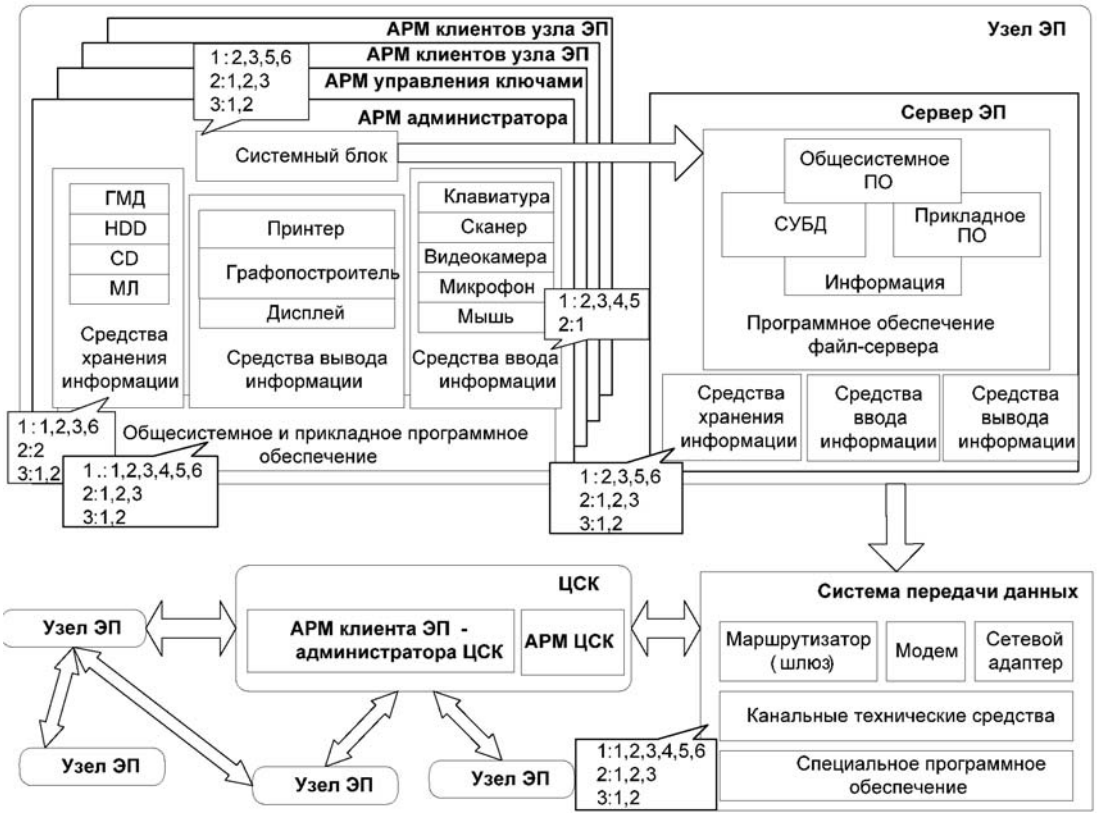

Рис. 2. Общая структура подсистемы защиты информации в ВПБС

Рис. 3. Структурная схема модели реализации угроз информационных ресурсов в ВПБС

компьютеров за выбранную единицу времени. Считаем, что D является константой на протяжении всех дальнейших вычислений, несмотря на различия в мощности и типах атакуемого вычислительного оборудования и пропускной способности каналов связи. Кроме того, вычисления делаются с учетом того, что один и тот же компьютер не может быть атакован дважды. Пусть $a(t)$ – пропорция уязвимых ПК, которые были успешно атакованы во время t, тогда $N \cdot a(t)$ – общее количество успешно атакованных компьютеров. Поскольку часть компьютеров уже была успешно атакована (их доля составляет $a(t)$), каждым новым захваченным компьютером будет произведено не более $D(1-a(t))$ новых успешных атак. Таким образом, количество захваченных компьютеров за период времени $d(t)$ равно (зафиксировав $a(t)$):

$$n = aN \cdot D(1-a)dt.$$

Учитывая, что N – константа, то $n = d(Na) = Nda$. Тогда верно следующее уравнение:

$$Nda = aN \cdot D(1-a)dt,$$

которое ведет к дифференциальному уравнению вида

$$\frac{da}{dt} = Da(1-a)$$

и имеет следующее решение:

$$a = \frac{e^{D(t-T)}}{1+e^{D(t-T)}},$$

где T является временным параметром, характеризующим наибольший рост атак.

На основании проведенных вычислений разработаем общую структуру подсистемы защиты информационных ресурсов в ВПБС.

2. ПОСТРОЕНИЕ ОБЩЕЙ СТРУКТУРЫ ПОДСИСТЕМЫ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВПБС

Для построения общей структуры подсистемы безопасности информационной безопасности ВПБС и моделей атак выбран функциональный тип математических моделей, называемый моделями «черного ящика». *Математическая модель* является моделью объекта, процесса или явления, представляющей собой математические закономерности, с помощью которых описаны основные характеристики моделируемого объекта, процесса или явления [5]. Данные модели построены в соответствии с методологиями IDEF0 и DFD с использованием CASE-средства BP-Win.

Для обеспечения защиты информации в системе электронного документооборота используется криптографический метод электронной цифровой подписи согласно стандартам, ратифицированным в Украине: ДСТУ-4145, ГОСТ 28147-89, ГОСТ 34310-95, ГОСТ 34311-95. Необходимо отметить, что цифровая подпись позволяет не только аутентифицировать автора электронного документа, но и подтвердить целостность последнего.

На рис. 4–5 приведена общая структура подсистемы защиты информационных ресурсов ВПБС. При этом под нарушителем безопасности понимается физическое лицо, случайно или преднамеренно совершающее действие, следствием которого является нарушение безопасности ВПБС.

На основании проведенного анализа угроз и построенной общей модели подсистемы защиты информационных ресурсов ВПБС рассмотрим модели активной и пассивных атак, которые могут быть реализованы в банковской системе. Общим для описания данных математических моделей является процесс формирования криптограммы.

Для этого зафиксируем конечное множество $I = \{I_1, I_2, \ldots, I_m\}$ пакетов, передаваемых в банковской транзакции, причем каждому пакету соответствует вероятность $P^*(I_j)$. Распределение вероятностей случайного процесса задается совокупным распределением вероятностей случайных величин, т. е. множеством вероятностей $P_o^* = \{P^*(I_1), P^*(I_2), \ldots, P(I_m)\}$ [6]. Источник ключей порождает поток ключей из множества K и/или K^*. Каждому ключу

Рис. 4. Общая структура подсистемы защиты информационных ресурсов ВПБС (контекстная диаграмма)

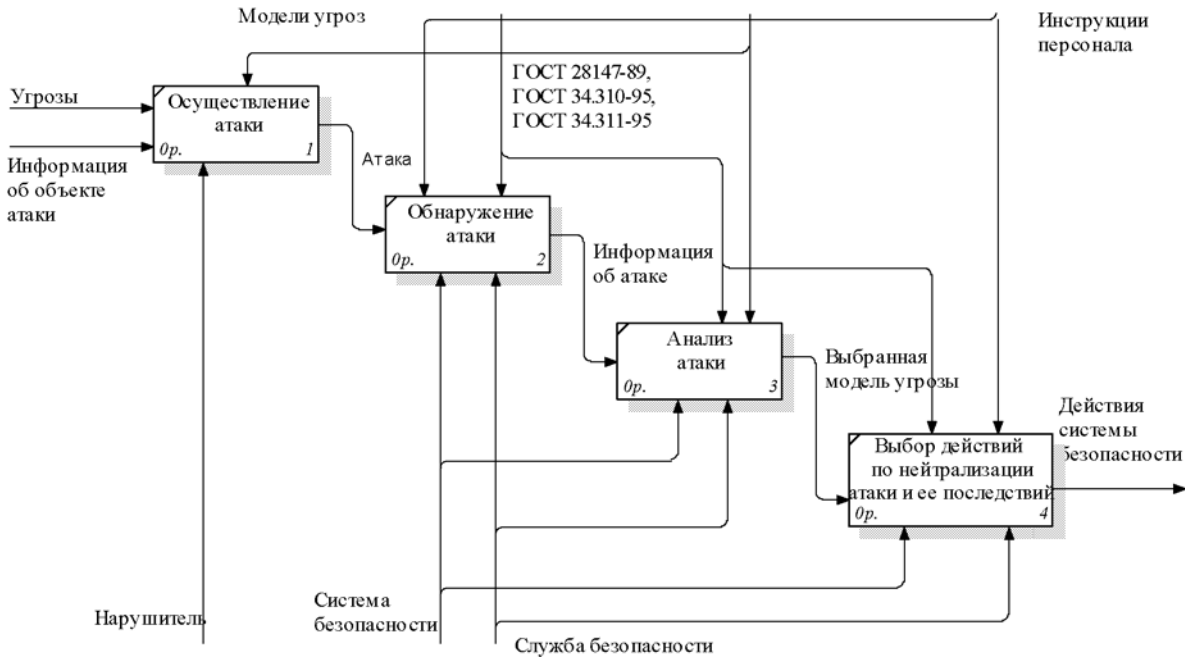

Рис. 5. Декомпозиция общей структуры подсистемы защиты информационных ресурсов

$K_i \in K = \{K_1, K_2, \ldots, K_k\}$ соответствует некоторая вероятность $P^*(K_i)$, а каждому $K_i^* \in K^* = \{K_1^*, K_2^*, \ldots, K_k^*\}$ соответствует вероятность $P^*(K^*_i)$. Случайный процесс выработки ключей задается множествами вероятностей:

$$P_K^* = \{P^*(K_1), P^*(K_2), \ldots, P^*(K_k)\};$$

$$P_{K^*}^* = \{P^*(K_1^*), P^*(K_2^*), \ldots, P^*(K_k^*)\}.$$

Выбор ключа K_i определяет конкретное отображение φ_i из множества отображений φ. С помощью отображения φ_i, соответствующего выбранному ключу K_i, по поступившему пакету i_j формируется криптограмма

$$E_l = \varphi_i(K_i, I_j).$$

Криптограмма E_l передается в точку приема по некоторому каналу. Последующие действия нарушителя определяются целью проведения атаки, а соответственно ее типом.

Отличие между активными и пассивными атаками заключается в том, что при выполнении атак первого типа (активные атаки) нарушитель осуществляет активные действия, т. е. действия, связанные с изменением потока данных либо с созданием фальшивых потоков (имитация, воспроизведение, модификация сообщений или помехи в обслуживании). Целью второго типа атак (пассивные атаки) является получение передаваемой информации (раскрытие содержимого сообщений и анализ потока данных).

Оценка степени эффективности атаки может быть осуществлена за счет проведения анализа данных, которыми владеет злоумышленник, анализа его возможностей и других параметров атаки. Основным методом оценки возможностей злоумышленника при атаке есть создание модели атаки. Рассмотрим основные модели атак на ВПБС.

3. ПОСТРОЕНИЕ МАТЕМАТИЧЕСКОЙ МОДЕЛИ ПАССИВНЫХ АТАК НА ВПБС

Пассивные угрозы вытекают из прослушивания (несанкционированного считывания информации) и не связаны с каким-либо изменением информации [6]. Суть атаки заключается в том, что нарушитель, определив факт выполнения криптографического протокола, перехватывает все данные, которые были переданы по каналу связи. То есть при передаче криптограммы E_l 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. Криптоанализ протокола зависит от типа протокола,

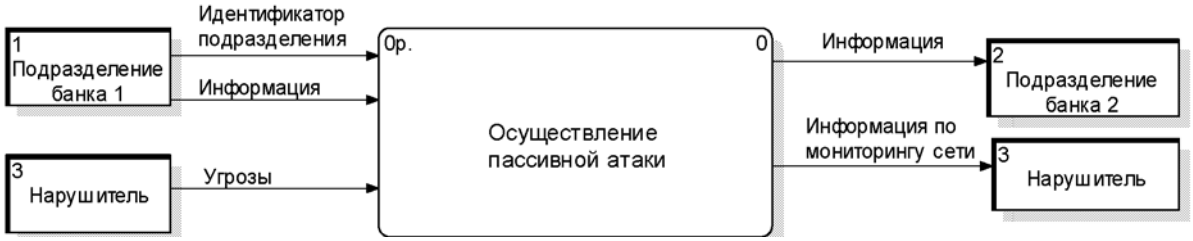

Рис. 6. Модель пассивных атак на информационные ресурсы во ВПБС

Рис. 7. Декомпозиция модели пассивных атак

количества и типа ключей, математического аппарата, который используются в протоколе, и других характеристик протокола.

На приемной же стороне с помощью обратного отображения φ_i^{-1} (заданного ключом K_i^*) из криптограммы E_l восстанавливается первоначальная информация

$$I_j = \varphi_i^{-1}(K_i^*, E_l).$$

Обобщенная модель пассивных атак представлена на рис. 6–7.

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. Рассмотрим основные типы активных атак.

4. ПОСТРОЕНИЕ МОДЕЛИ АКТИВНЫХ АТАК НА ВПБС С БЛОКИРОВКОЙ ПЕРЕДАЧИ ИНФОРМАЦИИ

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.

Обобщенная модель активных атак с блокировкой передачи информации представлена на рис. 8–9. Получателем информации в данной модели является нарушитель.

Таким образом, при реализации данной атаки необходимые данные не достигают пункта назначения, либо достигают слишком поздно, что приводит к потере конфиденциальной банковской информации.

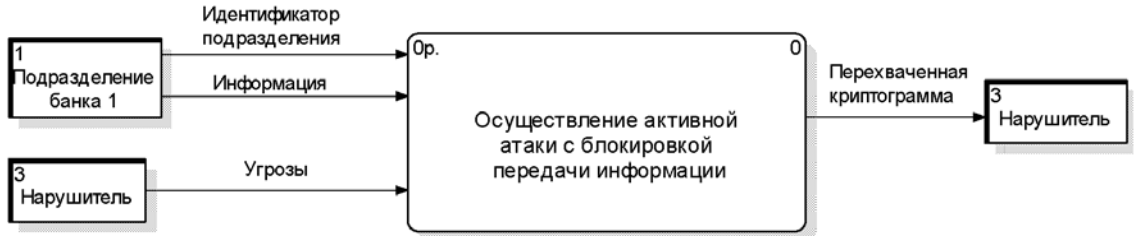

Рис. 8. Модель активных атак с блокировкой передачи информации

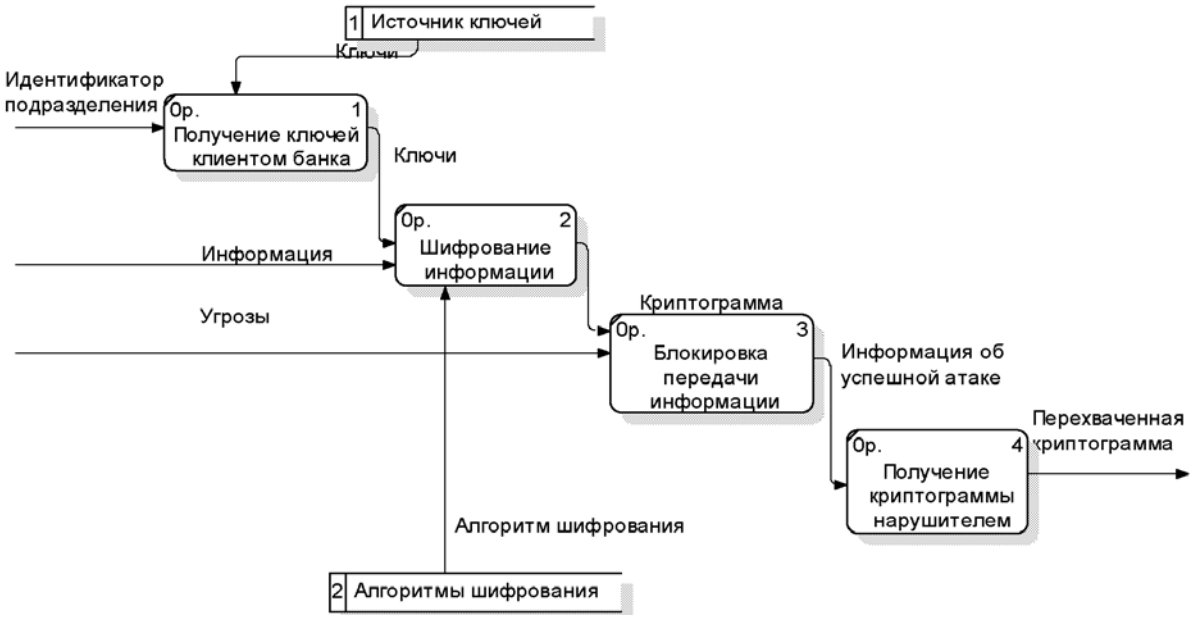

Рис. 9. Декомпозиция модели активных атак с блокировкой передачи информации

5. ПОСТРОЕНИЕ МОДЕЛИ АКТИВНЫХ АТАК НА ВПБС С ВНЕСЕНИЕМ ПОМЕХ

Суть атаки с внесением помех заключается в том, что нарушитель, определив факт выполнения криптографического протокола, вносит некоторую ошибку e и передает в точку приема криптограмму $(E_l + e)$. На приемном конце с помощью обратного отображения φ_i^{-1} (заданного ключом K_i^*) из криптограммы $(E_l + e)$ восстанавливается недостоверная информация

$$I_j^e = \varphi_i^{-1}(K_i^*, E_l + e),$$

т. е. подразделение банка получает сообщение, отличное от исходного $I_j^e \neq I_j$.

Обобщенная модель активных атак с внесением помех представлена на рис. 10–11.

Реализация данной атаки может привести к сбою или к получению на приемной стороне ложной транзакции. Таким образом, нарушитель может «руководить» банковскими активами и конфиденциальной информацией банка.

6. ПОСТРОЕНИЕ МОДЕЛИ АКТИВНЫХ АТАК «МАСКАРАД» НА ВПБС

Суть атаки «маскарад» заключается в том, что пользователь (или иная сущность – процесс, подсистема и т. д.) 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.

Рассмотрим процесс выполнения атаки данного типа. Нарушитель, определив факт выполнения криптографического протокола, перехватывает криптограмму E_l. С ее помощью он может попытаться вычислить апостериорные вероятности различных возможных сообщений:

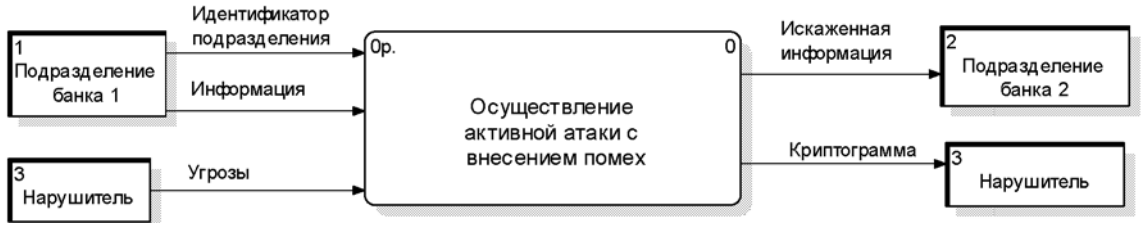

Рис. 10. Модель активных атак с внесением помех

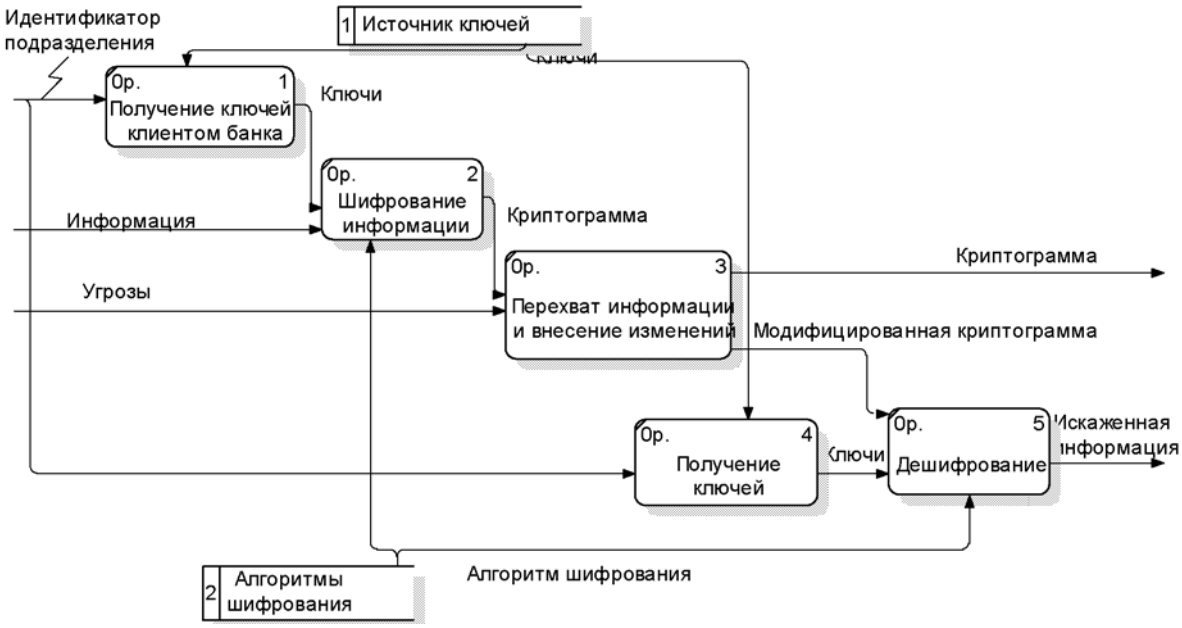

Рис. 11. Декомпозиция модели активных атак с внесением помех

$$P^*_{o|E_l} = \{P^*(I|_1E_l), P^*(I_2|E_l), \ldots, P^*(I_m|E_l)\}$$

и различных возможных ключей:

$$P^*_{K|E_l} = \{P^*(K_1|E_l), P^*(K_2|E_l), \ldots, P^*(K_k|E_l)\},$$

которые могли быть использованы при формировании криптограммы E_l.

Множества апостериорных вероятностей образуют апостериорные знания нарушителя о ключах $K = \{K_1, K_2, \ldots, K_k\}$ и об информации $I = \{I_1, I_2, \ldots, I_m\}$ после перехвата криптограммы E_l. Фактически, множества $P^*_{K|E_l}$ и $P^*_{M|E_l}$ представляют собой множества предположений, которым приписаны соответствующие вероятности.

Затем, получив необходимую информацию, нарушитель формирует криптограмму с недостоверной информацией

$$E^e_l = \varphi_i(K_i, I^e_j)$$

и передает ее в точку приема.

На приемном конце с помощью обратного отображения φ_i^{-1} (заданного ключом K^*_i) из криптограммы E^e_l восстанавливается недостоверная информация, переданная нарушителем:

$$I^e_i = \varphi_i^{-1}(K^*_i, E^e_l), \; I^e_j \neq I_j.$$

Такого типа атака, как правило, связана с попытками проникновения внутрь периметра безопасности ВПБС и часто реализуется хакерами.

Обобщенная модель активных атак «маскарад» представлена на рис. 12–13.

Наиболее опасен «маскарад» в банковских системах электронных платежей, где неправильная идентификация клиента может привести к потере его конфиденциальной информации и активов.

Анализ рассмотренных атак показывает, что любая реализованная активная атака приводит к потере конфиденциальной информации (банка или его клиентов) и наносит экономический ущерб, как активам банка, так и активам его клиентов. Реализация

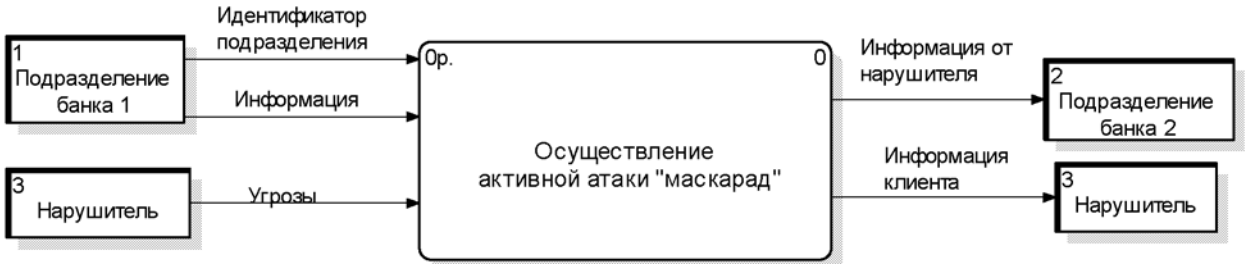

Рис. 12. Модель активных атак «маскарад»

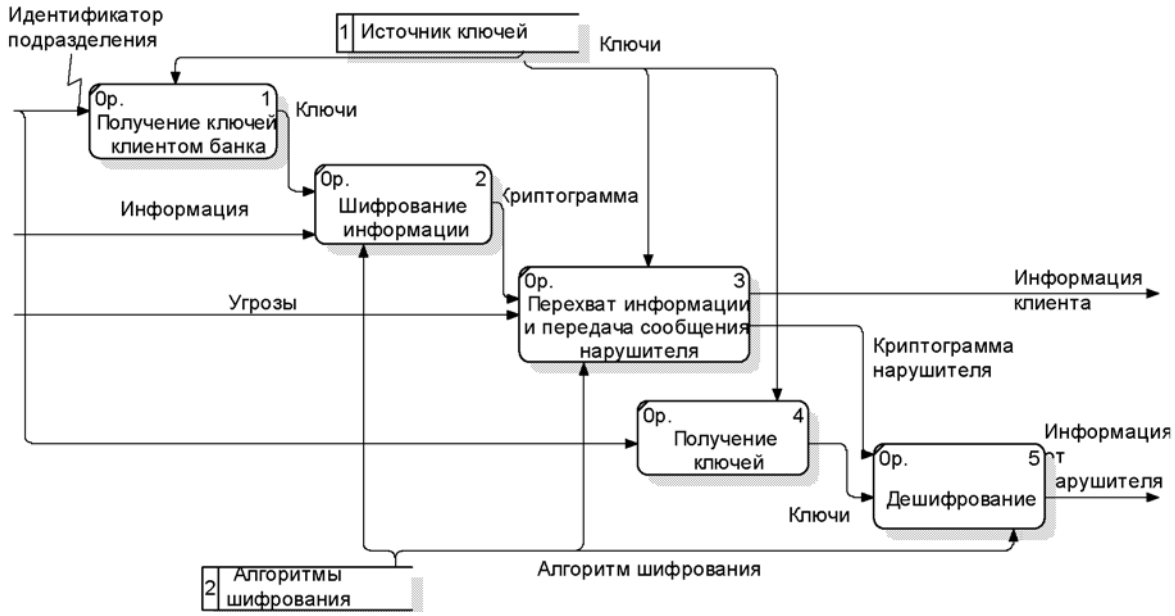

Рис. 13. Декомпозиция модели активной атаки «маскарад»

пассивной атаки может привести к потере «конфиденциальности» передаваемой транзакции, что дает возможность нарушителю на основе полученной информации реализовать активную атаку.

7. ОПРЕДЕЛЕНИЕ ОСНОВНЫХ НАПРАВЛЕНИЙ ЗАЩИТЫ ВПБС

Для предотвращения угроз на информационные ресурсы ВПБС рассмотрим основные направления защиты банковской информации, представленные на рис. 14.

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 алгоритма защиты, высокая стоимость реализации криптоалгоритма.

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, а также возможность упрощения или усложнения применяемых криптографических методов, в зависимости от потребностей обеспечения безопасности. На рис. 15 приведена взаимосвязь основных направ-

Рис. 14. Основные направления защиты информации

Рис. 15. Взаимосвязь направлений и средств защиты ВПБС

лений и средств защиты информационных ресурсов в ВПБС.

Проведенный анализ рис. 14 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; программную реализацию выбранных криптографических алгоритмов.

ВЫВОДЫ

Таким образом, проведенные исследования показали, что для обеспечения безопасности банковской информации в ВПБС используются криптографические

симметричные и асимметрические алгоритмы шифрования, обеспечивающие аутентичность и целостность сообщений. Разработанные математические модели позволяют оценить степень эффективности основных типов атак, что облегчает выбор необходимых средств и методов защиты информации в ВПБС. Перспективным направлением дальнейших исследований является разработка методики оценки экономического ущерба, нанесенного в результате реализации угроз на информационные ресурсы ВПБС.

СПИСОК ЛИТЕРАТУРЫ

1. Украинский ресурс по безопасности [Электронный ресурс]. – Электрон. дан. – Режим доступа: http://kiev-security.org.ua. – Загл. с экрана.
2. Дело [Электронный ресурс]. – Электрон. дан. – Режим доступа: http://delo.ua/wiki/Glossary/vnutribankovskaja-platezhnaja-sistema-130342. – Загл. с экрана.
3. *Кузнецов А. А.* Анализ механизмов обеспечения безопасности банковской информации во внутриплатежных системах коммерческого банка / А. А. Кузнецов, О. Г. Король, А. М. Ткачов // Матеріали І міжнародної науково-практичної конференції «Безпека та захист інформації в інформаційних і телекомунікаційних системах», 28–29 травня 2008 р. Зб. наук. статей «Управління розвитком». – Х. : ХНЕУ, 2008. – № 6. – С. 28–35.
4. *В. Столлингс.* Криптография и защита сетей: принципы и практика : пер. с англ. – 2-е изд. – М. : Вильям, 2001. – 672 с.
5. Глоссарий [электронный ресурс]. – Электрон. дан. – Режим доступа: http://www.glossary.ru. – Загл. с экрана.
6. *Кузнецов О. О.* Захист інформації та економічна безпека підприємства : монография / О. О. Кузнецов, С. П. Євсеєв, С. В. Кавун. – Х. : ХНЕУ, 2008. – 360 с.

Надійшла 08.09.2009

Євсеєв С. П., Король О. Г., Гончарова А. І.

ПОБУДОВА МОДЕЛЕЙ АТАК НА ВНУТРІШНЬОПЛАТІЖНІ БАНКІВСЬКІ СИСТЕМИ

Аналізуються погрози інформаційних даних у внутрішньоплатіжних банківських системах (ВПБС). Розробляються модель реалізації погроз інформаційних даних у ВПБС, математичні моделі пасивної і активної атак, досліджуються основні напрями захисту у ВПБС.

Ключові слова: погрози, внутрішньоплатіжна банківська система, математична модель, модель реалізації погроз, пасивна атака, активна атака, захист, шифрування, автентичність, цілісність.

Evseev S. P., Korol O. G, Goncharova A. I.

MODEL-BUILDING OF ATTACKS ON INTERNAL-PAYMENT BANKING SYSTEM

Threats to information data in an internal-payment banking system (IPBS) are being analyzed. The realization model of information data threats in IPBS as well as the mathematical models of passive and active attacks are being developed. The general protection areas in IPBS are being studied.

Key words: threats, internal-payment banking system, mathematical model, realization model of threats, passive attack, active attack, protection, encoding, authenticity, integrity.

УДК 621.391

Калекина Т. Г.[1], Коваленко Т. Н.[2]

[1]Канд. техн. наук, доцент Харьковского национального университета радиоэлектроники

[2]Канд. техн. наук, доцент Харьковского национального университета радиоэлектроники

ОБОСНОВАНИЕ КРИТЕРИЯ СТРУКТУРНО-ИНФОРМАЦИОННОЙ СВЯЗНОСТИ ПРИ АНАЛИЗЕ НАДЕЖНОСТИ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ И СЕТЕЙ

В работе предложены комплексные показатели надежности телекоммуникационных систем и сетей, учитывающие одновременно как структурные, так и функциональные характеристики сети. Предложенные показатели позволяют оценить не только потенциальную надежность телекоммуникационной сети – верхнюю границу структурной надежности, но и надежность сети с учетом ограниченной пропускной способности каналов.

Ключевые слова: надежность, структурная связность, информационная связность, интегральный показатель, граф, телекоммуникационная сеть.

Вопросы анализа надежности сложных разветвленных телекоммуникационных систем и сетей (ТКС) всегда были в центре внимания проектировщиков перспективных систем связи. Под структурной надежностью сети связи понимается объективное свойство сети обеспечивать связность пользователей сети с качеством не хуже заданного. Без средств анализа надежности ТКС отдел информационных технологий предприятия не сможет ни проконтролировать, ни тем более обеспечить необхо-