ОПРЕДЕЛЕНИЕ КЛАССА ЗАЩИТЫ ИНФОРМАЦИИ ОТДЕЛА ОПЕРАЦИЙ С БАНКОВСКИМИ КАРТОЧКАМИ

DETERMINING THE INFORMATION SECURITY CLASS OF THE BANK CARD OPERATIONS DEPARTMENT

УДК 004.056

Акулов Артем Алексеевич, магистрант, Донской государственный технический университет, г. Ростов-на-Дону

Akulov A.A. artkulov_ww@mail.ru

Аннотация

Работа посвящена описанию объекта защиты информации, а именно отдела операций с банковскими карточками. В ней приводятся виды и источники угроз, классы каналов несанкционированного получения информации, потенциально возможные действия злоумышленника. На основе анализа полученной информации необходимо выбрать требуемый класс защиты информации.

Annotation

The work is devoted to the description of the object of information protection, namely, the department of operations with bank cards. It lists the types and sources of threats, classes of channels for unauthorized information acquisition, and potentially possible actions of an attacker. Based on the analysis of the received information, it is necessary to select the required information security class.

Ключевые слова: информационная безопасность, угрозы, класс защиты информации, несанкционированное получение информации.

Keywords: information security, threats, information security class, unauthorized receipt of information.

С момента появления банков они неизменно вызывали интерес преступников. Интерес этот был связан не только с деньгами, которые там хранятся, но и с тем, что в банках находится важная и зачастую носящая секретный характер информация о финансово-хозяйственной деятельности многих людей, компаний, организаций и даже целых государств.

Информационная безопасность (ИБ) – процесс обеспечения конфиденциальности, целостности и доступности информации. Одной из основных целей для специалистов в области ИБ является процесс обеспечения защиты информации. Данный процесс можно реализовать с помощью различных программно-аппаратных средств. При этом программное обеспечение (ПО) участвует в оптимизации работы системы в целом, а не только для выполнения её основных функций.

Одним из важнейших этапов обеспечения ИБ на предприятии является анализ и выявление всех возможных угроз для данной системы. Из этого следует, что разрабатываемая система защиты при выявлении тех или иных угроз будет отличатся.

В настоящее время в связи с приходом информатизации и компьютеризации банковской деятельности значение ИБ банков многократно возросло, на сегодняшний день в результате увеличения количества электронных платежей, пластиковых карт и компьютерных сетей, деньги банков и их клиентов стали объектом информационных атак. Совершить такую атаку может любой – достаточно лишь наличия компьютера с подключением к сети Интернет. Причем для осуществления такой атаки нет необходимости физического проникновения в банк, все можно реализовать удаленно даже за тысячи километров от цели.

Компьютеризация банковской деятельности значительно повысила производительность труда сотрудников банка, внедрила новые финансовые продукты и технологии. Однако развитие техники для преступлений шло не менее

быстрыми темпами, чем развитие банковских технологий. Сейчас большинство преступлений в банковской системе (БС) связаны с использованием автоматизированных систем обработки информации банка (АСОИБ). Из этого следует, что банкам при ее создании и модернизации необходимо учитывать все аспекты ее безопасности. Именно этой проблеме посвящена данная статья.

Организация защиты АСОИБ представляет собой единый комплекс мер, направленных на учет всей специфики процесса обработки информации. Несмотря на то, что у пользователя могут возникнуть какие-либо неудобства в процессе работы, в большинстве случаях система защиты может оказаться совершенно необходимой для нормального функционирования комплекса.

Любой современный банк не может обойтись без компьютерных систем (КС), которые представляют собой источник совершенно новых, ранее неизвестных угроз.

Организация ИБ банковских отделов достаточно сильно отличается от организации других компаний и организаций. Причиной того является прежде всего специфический характер угроз, а также публичная деятельность банков, которая вынуждает облегчить доступ к счетам для повышения удобства для клиентов.

Простая компания старается главным образом защитить информацию от конкурентов и поэтому строит свою ИБ, на основе узкого круга потенциальных угроз. Такая информация может представлять интерес только для узкого круга лиц и организаций и редко является ликвидной, т.е. может быть конвертирована в денежную форму.

ИБ банковского отдела должна учитывать следующие специфические факторы.

1. Вся информация, хранящаяся в БС, – это реальные деньги. На основе этой информации можно производить платежи, открывать кредиты и переводить значительные суммы. Очевидно, что незаконное манипулирование такой информацией может привести к серьезным потерям. Эта особенность резко расширяет круг преступников, покушающихся на банки.

2. Информация в БС затрагивает интересы большого количества людей и разных организаций, являющимися клиентами банка. Как правило, такая информация конфиденциальна, и банк несет полную ответственность за обеспечение требуемого уровня секретности для своих клиентов. Естественно, у клиентов должна быть уверенность, что банк заботится об их интересах, иначе он рискует своей репутацией со всеми вытекающими отсюда последствиями.

3. Удобство работы клиента с банком, спектр предоставляемых услуг, в том числе услуги удаленного доступа, сильно влияют на конкурентоспособность банка. Поэтому клиент должен иметь возможность быстро и без утомительных процедур распорядиться своими деньгами. Однако такая легкость значительно повышает вероятность преступного проникновения в БС.

4. ИБ банка (в отличие от большинства компаний) должна обеспечивать высокую надежность работы КС даже в случае чрезвычайных ситуаций, поскольку банк несет ответственность не только за собственные средства, но и за деньги клиентов.

Исследуемый объект защиты информации представляет собой компьютер с соответствующим программно-аппаратным обеспечением для осуществления действий с банковскими пластиковыми картами. Как и любой другой, исследуемый нами объект состоит из нескольких подсистем, в каждой из которых существуют различные угрозы.

1 Виды и источники угроз

В подсистеме управления доступа возможны такие угрозы как:

– получение доступа к системе посредством кражи пароля;

– кража конфиденциальной информации на съемный носитель личного пользования;

– установка и использование нелицензионного программного обеспечения (ПО).

В подсистеме регистрации и учета:

– ошибки пользователя;

– вредоносное ПО;

– кража данных в печатном виде;

– кража съемных носителей, использующихся в пределах банка;

– съем информации с освобождаемых областей оперативной памяти электронно-вычислительной машины (ЭВМ) и внешних накопителей.

В криптографической подсистеме:

– кража информации в различных каналах связи;

– получение злоумышленником криптографического ключа.

В подсистеме обеспечения целостности:

– нарушение целостности обрабатываемой информации;

– доступ злоумышленника к различным устройствам и носителям информации.

2 Каналы несанкционированного получения информации

Существующие каналы несанкционированного получения информации:

– побочные электромагнитные излучения и наводки;

– линии и каналы передачи данных;

– акустические каналы (распространение звуковых колебаний в любом звукопроводящем материале);

– электрические каналы (опасные напряжения и токи в различных токопроводящих коммуникациях).

3 Возможные действия злоумышленника

Возможные действия злоумышленника:

– несанкционированный доступ в помещение;

– возможность записи информации на переносные устройства (флэш-накопители, CD- и DVD-диски и т.п.);

– пересылка фотоснимков бумажных носителей и экранов мониторов с помощью мобильных телефонов и другими способами, через удаленный доступ к ПК;

– программные вирусы и «троянские» программы;

– кража внутреннего накопителя информации (жесткого диска);

– кража бумажных документов;

– использование знаний в области социальной инженерии для получения конфиденциальной информации;

– проникновение в банк и установка звукозаписывающих устройств («жучков»);

4 Требуемый класс защиты информации

Для определения требуемого класса защиты информации необходимо определить требования работы с автоматизированной системой (АС).

В подсистеме контроля доступом:

– субъекты доступа должны быть идентифицированы и аутентифицированы при входе в систему с использованием идентификатора (кода), а также условно-постоянного пароля имеющего длину не меньше шести буквенно-цифровых символов;

– терминалы, компьютеры, устройства в компьютерной сети, каналы связи, внешние компьютерные устройства должны быть идентифицированы по их логическим адресам (номерам);

– программы, тома, каталоги, файлы, записи и поля записей должны быть идентифицированы по имени;

– должно быть управление потоками информации с использованием меток конфиденциальности.

В подсистеме регистрации и учета:

– необходимо осуществлять регистрацию входа (выхода) субъектов доступа в систему (из системы), или регистрировать загрузки и инициализации

операционной системы и ее программное выключение. В моменты аппаратурного отключения АС регистрация выхода из системы или останова не осуществляется

– выдача печатных (графических) документов должна регистрироваться на "твердую" копию. Во время выдачи каждый лист (страница) документа должен автоматически маркироваться порядковым номером и учетными реквизитами АС с указанием общего количества листов (страниц) на последнем листе документа;

– запуск (завершение) различных программ или процессов (заданий, задач), используемых для обработки защищаемых файлов должны регистрироваться;

– попытки доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам должна регистрироваться;

– должна производиться запись всех защищаемых носителей информации путем их маркировки и занесения учетных данных в журнал (учетную карточку);

В криптографической подсистеме:

– вся конфиденциальная информация, записываемая на совместно используемые различными субъектами доступа (разделяемые) носители данных и в каналах связи должна шифроваться;

– операции шифрования и криптографические ключи должны дополнительно контролироваться подсистемой контроля доступом;

– необходимо использовать сертифицированные средства криптографической защиты.

В подсистеме обеспечения целостности:

– целостность СЗИ НСД проверяется при загрузке системы наличием имен (идентификаторов) компонентов СЗИ;

– должен быть администратор (служба) защиты информации, ответственный за поддержание, нормальную работу и мониторинг работы СЗИ НСД;

– должны быть доступны средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и периодическое обновление и мониторинг их работоспособности;

– необходимо использовать сертифицированные средства защиты. Их сертификация осуществляется специальными сертификационными центрами или специализированными предприятиями, имеющими лицензию на сертификацию средств защиты СЗИ НСД.

На основе вышеприведенных требований, видов и источников угроз и каналов несанкционированного получения информации, а также классификатору, находящемуся в руководящем документе от 30 марта 1992 г. «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», данному объекту разумно присвоить класс защищенности – 2А.

Литература

1. Тютюнник А.В., Шевелев А.С. Информационные технологии в банке - Издательская группа «БДЦ-пресс». - 2003 г.
2. Киселева И.А. Коммерческие банки: модели и информационные технологи в процедурах принятия решений. - М.: Едиториал УРСС, 2002. - 400 с.
3. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации Решение председателя Гостехкомиссии России от 30 марта 1992 г.
4. Факторы, влияющие на требуемый уровень защиты [Электронный ресурс]. – Режим доступа: https://studfiles.net/preview/3657038/page:2/

Literature

1. Tyutyunnik A.V., Shevelev A. S. Information technologies in the bank - Publishing group "BDC-press". - 2003
2. Kiseleva I. A. Commercial banks: models and information technologies in decision-making procedures. - Moscow: Editorial URSS, 2002. - 400 p.

3. Guidance document. Automated systems. Protection against unauthorized access to information. Classification of automated systems and requirements for information protection Decision of the Chairman of the State Technical Commission of Russia of March 30, 1992
4. Factors affecting the required level of protection [Electronic resource]. - Access mode: https://studfiles.net/preview/3657038/page:2/