УДК 336.7

Тремасова Наталья, *студентка 4 курса специальности «Экономическая безопасность» ФГБОУ ВПО «Мордовский государственный университет им. Н.П. Огарёва»*

Москалёва Елена Геннадьевна, *кандидат экономических наук, доцент кафедры бухгалтерского учета, анализа и аудита ФГБОУ ВПО «Мордовский государственный университет им. Н.П. Огарёва»*

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КОММЕРЧЕСКОГО БАНКА (НА ПРИМЕРЕ АККСБ «КС БАНК»)

Аннотация: В статье раскрывается сущность информационной безопасности на примере кредитной организации АККСБ «КС БАНК». Также рассматриваются угрозы и риски, связанные с утечкой информации, защита информации. Предложен механизм совершенствования информационной безопасности банка.

Ключевые слова: информация, информационная безопасность, угрозы, ущерб, средства защиты информации.

Annotation: The article reveals the essence of information security on the example of a credit institution AKKSB "KS BANK". It also discusses the threats and risks associated with information leakage, information security. The mechanism of improving the information security of the bank.

Keywords: information, information security, threats, damage data protection.

Информация – такая же составляющая любого бизнеса, как производственное оборудование, конкретные люди, на которых держится производство, выстроенные отношения с заказчиками и поставщиками и т. д. С этим невозможно спорить. Потеря, порча или сбой в функционировании любой из названных составляющих бизнеса приводит к последствиям, лежащим в диапазоне от «нанесения ущерба» до «закрытия бизнеса». И сейчас вопрос безопасности данных регулируется государственными законами.

Любое предприятие располагает различными видами информации, которые представляют интерес для злоумышленников. Прежде всего к ней относятся:

коммерческие данные, информация, являющаяся интеллектуальной собственностью предприятия и конфиденциальные данные.

И если производственное оборудование охраняет служба безопасности предприятия, ценных специалистов «бережет» продуманная кадровая политика, то кто и как занимается вопросами информационной безопасности (ИБ) предприятия?

В реальности существует два вида угроз информационной безопасности [1]:

- внешние - несанкционированный доступ из сети Интернет; снятие информации с кабельных систем (ЛВС и электропитания) при помощи технических средств; запись разговоров на расстоянии сквозь стены (окна, двери) и т. д.;

- внутренние - несанкционированный доступ в помещение; несанкционированный и неизбирательный доступ к данным внутри корпоративной сети; 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; программные вирусы и «троянские» программы, не контролируемая электронная почта и т. д.

Теоретически все угрозы информационной безопасности предприятия можно разделить на два больших блока [5]:

1. Группа злоумышленных воздействий. Сюда относятся действия каких-либо лиц или организаций, которые имеют целью нанесение ущерба благосостоянию деятельности информационного обеспечения предприятия. В том числе, промышленный шпионаж и подрыв ситуации.

2. Группа незлоумышленных воздействий. К ним можно отнести отсутствие должного внимания или же упущение различного рода поступающей информации со стороны аналитиков.

К числу причин, подрывающих информационную безопасность предприятия относятся:

- плохая организация работы информационной службы;

- недостаточное финансирование;

- нечеткое формулирование задач анализа;

- плохое взаимодействие подразделений предприятия.

Практика показывает, что совокупный ущерб экономической безопасности предприятий от внутренних негативных воздействий во много раз превосходит ущерб от внешних, приводя к банкротству предприятий, позволявших себе недостаточное внимание уделять анализу поступающей информации, поэтому проблема качественная организация обеспечения информационной безопасности деятельности предприятия представляется жизненно важным для ее безопасного и успешного функционирования.

Действие угроз информационной безопасности объекта направлено на создание возможных каналов утечки защищаемой информации (предпосылок к ее утечке) и непосредственно на утечку информации. Одно из ключевых понятий в оценке эффективности проявления угроз объекту информационной безопасности — ущерб, наносимый этому предприятию в результате воздействия угроз.[6]

По своей сути любой ущерб, его определение и оценка имеют ярко выраженную экономическую основу. Не является исключением и ущерб, наносимый информационной безопасности предприятия.

С позиции экономического подхода общий ущерб информационной безопасности предприятия складывается из двух составных частей: прямого и косвенного ущерба.

Прямой ущерб информационной безопасности предприятия возникает вследствие утечки конфиденциальной информации. Косвенный ущерб — потери, которые несет предприятие в связи с ограничениями на распространение информации, в установленном порядке отнесенной к категории конфиденциальной.[4]

Обеспечение безопасности является неотъемлемой составной частью деятельности банка. Состояние защищенности представляет собой умение и способность надежно противостоять любым попыткам криминальных структур или недобросовестных конкурентов нанести ущерб законным интересам банка.[1]

Безопасное состояние дел в банке способно обеспечить успешную деятельность банка, получение запланированного дохода, надежное положение и рациональное позиционирование банка на рынке, положительные результаты при сегментировании предлагаемых для клиентов услуг. Вместе с тем безопасность означает также достижение условий, позволяющих предотвращать влияние угроз и воздействие опасностей, что обеспечивает надлежащую организацию защиты банка.

Информационная безопасность и защита информации банка должны быть на достаточно высоком уровне, чтобы отражать любые атаки и попытки вторжения со стороны злоумышленников, в том числе со стороны сотрудников самой организации.

Информационная безопасность банка учитывает следующие специфические факторы [3]:

1. Хранимая и обрабатываемая в банковских системах информация представляет собой реальные деньги. На основании информации компьютера могут производиться выплаты, открываться кредиты, переводиться значительные суммы. Вполне понятно, что незаконное манипулирование с такой информацией может привести к серьезным убыткам. Эта особенность резко расширяет круг преступников, покушающихся именно на банки (в отличие от, например, промышленных компаний, внутренняя информация которых мало кому интересна).

2. Информация в банковских системах затрагивает интересы большого количества людей и организаций — клиентов банка. Как правило, она конфиденциальна, и банк несет ответственность за обеспечение требуемой степени секретности перед своими клиентами. Естественно, клиенты вправе ожидать, что банк должен заботиться об их интересах, в противном случае он рискует своей репутацией со всеми вытекающими отсюда последствиями.

3. Конкурентоспособность банка зависит от того, насколько клиенту удобно работать с банком, а также насколько широк спектр предоставляемых услуг, включая услуги, связанные с удаленным доступом. Поэтому клиент должен иметь возможность быстро и без утомительных процедур распоряжаться

своими деньгами. Но такая легкость доступа к деньгам повышает вероятность преступного проникновения в банковские системы.

4. Информационная безопасность банка (в отличие от большинства компаний) должна обеспечивать высокую надежность работы компьютерных систем даже в случае нештатных ситуаций, поскольку банк несет ответственность не только за свои средства, но и за деньги клиентов.

5. Банк хранит важную информацию о своих клиентах, что расширяет круг потенциальных злоумышленников, заинтересованных в краже или порче такой информации.

К числу угроз информационным ресурсам АККСБ «КС Банк» относятся:

- разглашение конфиденциальной информации;

- утечка конфиденциальной информации через технические средства обеспечения производственной деятельности различного характера и исполнения;

- несанкционированный доступ к охраняемым сведениям со стороны конкурентных организаций и преступных формирований.

В связи с этими угрозами кредитная организация выделяет следующие объекты, подлежащие защите от потенциальных угроз и противоправных посягательств [1]:

- персонал Банка (руководящие работники, производственный персонал, имеющий непосредственный доступ к финансам, валюте, ценностям, хранилищам, осведомленные в сведениях, составляющих банковскую и коммерческую тайну, работники внешнеэкономических служб и другие);

- финансовые средства, валюта, драгоценности;

- информационные ресурсы с ограниченным доступом, составляющие служебную и коммерческую тайну, а также иная конфиденциальная информация на бумажной, магнитной, оптической основе, информационные массивы и базы данных, программное обеспечение, информативные физические поля различного характера;

- средства и системы информатизации (автоматизированные системы и вычислительные сети различного уровня и назначения, линии телеграфной,

телефонной, факсимильной, радио и оптической связи, технические средства передачи информации, средства размножения и отображения информации, вспомогательные технические средства и системы);

- материальные средства (здания, сооружения, хранилища, техническое оборудование, транспорт и иные средства);

- технические средства и системы охраны и защиты материальных и информационных ресурсов.

Таблица 1. «Риск и ущерб утечки информации»

Утечка информации	Риск	Ущерб
Внутренние регламенты банка	- опасность ограбления и мошенничества; - уход клиентов по причине разглашения персональных данных	финансовые потери
Условия обслуживания VIP-клиентов	потеря целевых клиентов	финансовые потери, ухудшение репутации
Персональные данные	- иски в суд со стороны клиентов по закону ФЗ №152 «О персональных данных»; - проверки со стороны регулирующих органов (ФСТЭК, ФСБ, Роскомнадзор)	финансовые потери, потеря клиента
Планы вывода нового продукта на рынок	конкурент выпускает новый продукт быстрее	потеря рынка
Финансовая информация	-снижение инвестиционной привлекательности; - пристальное внимание аудиторов	финансовые потери, штрафные санкции
Сведения по агентам, партнерам и условиям сотрудничества	конкурент предлагает более выгодные условия сотрудничества	потеря лучших бизнес-партнеров

Большинство информации содержится на компьютере, поэтому обеспечению технического аспекта информационной безопасности АККСБ «КС Банк» уделяется большое внимание. Оттого, насколько хорошо защищена информация, зависит эффективность безопасности банка.

Защита информации является составной частью банковской деятельности. Система обеспечения безопасности информационных ресурсов предусматривает комплекс организационных, технических, программных и криптографических средств и мер по защите информации в процессе традиционного документооборота при работе исполнителей с конфиденциальными документами и сведениями, при обработке информации в автоматизированных

системах различного уровня и назначения, при передаче по каналам связи, при ведении конфиденциальных переговоров. [1]

Вся совокупность технических средств в кредитной организации АККСБ «КС Банк» подразделяется на физические и аппаратные. Физические средства включают инженерные устройства и сооружения, препятствующие физическому проникновению злоумышленников на объекты защиты и осуществляющие защиту персонала (личные средства безопасности), материальных средств и финансов, информации от противоправных действий. К таковым относятся: замки на дверях, решетки на окнах, средства электронной охранной сигнализации и др.

Аппаратные средства – это устройства, встраиваемые непосредственно в вычислительную технику или устройства, которые сопрягаются с ней по стандартному интерфейсу.[2]

Управление доступом – это средство защиты информации регулированием использования всех ресурсов информационных систем и технологий. Оно должно противостоять всем возможным путям несанкционированного доступа к информации. Управление доступом включает следующие функции защиты:

1) идентификацию пользователей, персонала и ресурсов системы (присвоение каждому объекту персонального идентификатора);

2) опознание (установление подлинности) объекта или субъекта по предъявленному им идентификатору;

3) разрешение и создание условий работы в пределах установленного регламента;

4) регистрация (протоколирование) обращений к защищаемым ресурсам;

5) реагирование (сигнализация, отключение, задержка работ, отказ в запросе и т.п.) при попытках несанкционированных действий.

Программные средства – это специальные программы и программные комплексы, предназначенные для защиты информации в информационной системе. Из средств программного обеспечения системы защиты выделяют программные средства, реализующие механизмы шифрования (криптографии).[4]

Криптография – это наука об обеспечении секретности и (или) аутентичности (подлинности) передаваемых сообщений. Механизмы шифрования применяются как при обработке, так и при хранении информации на магнитных носителях. При передаче информации по каналам связи большой протяженности этот метод является единственно надежным.

К работе с криптографическими системами допускаются только сотрудники Банка, имеющие соответствующее разрешение от руководства Банка. [1]

Секретные ключи электронно-цифровых подписей и шифрования хранятся в сейфах под ответственностью лиц на то уполномоченных. Доступ неуполномоченных лиц к носителям секретных ключей и шифрования исключен.

Категорически запрещается:

- выводить секретные ключи и шифрования на дисплей компьютера или принтер;

- устанавливать в дисковод компьютера носитель секретных ключей и шифрования в непредусмотренных режимах функционирования;

- записывать на носитель секретных ключей и шифрования постороннюю информацию;

При компрометации секретных ключей, шифрования и прочей электронной информации Управлением банковских и информационных технологий принимаются меры для прекращения любых операций с использованием этих ключей и прочей информации; принимаются меры для смены ключей и шифрования, паролей. По факту компрометации организуется служебное расследование, результаты которого отражаются в акте и доводятся до сведения руководства Банка. [1]

Противодействие атакам вредоносных программ предполагает в первую очередь использование антивирусных программ, а также комплекс разнообразных мер организационного характера.

Организационные средства подразумевают регламентацию производственной деятельности в информационной системе и взаимоотношений

исполнителей на правовой основе таким образом, что разглашение, утечка и несанкционированный доступ к конфиденциальной информации становятся невозможным или существенно затрудняются за счет проведения организационных мероприятий. [4]

Морально-этические средства защиты включают всевозможные нормы поведения, которые традиционно сложились ранее, складываются по мере распространения информационных систем и технологий в стране и в мире или специально разрабатываются. Нормы морали могут быть неписаными (например, честность) либо оформленными в некий свод (устав) правил или предписаний. Эти нормы, как правило, не являются законодательно утвержденными, но поскольку их несоблюдение приводит к падению престижа организации, они считаются обязательными для исполнения. [4]

В целом информационная безопасность АККСБ «КС Банк» находится на низком уровнем. Большинство положений основывается на Общей концепции информационной безопасности банка. Что касается сотрудников, занимающихся проблемами информационной безопасности, то их не так много, всего лишь 5% из общей численности штата предприятия. Комплекс организационных мероприятий немного отстает от должного уровня. И только технические средства защиты информации являются сильным преимуществом кредитной организации, т.к. именно они обеспечивают наиболее эффективную защиту.

В связи с этим необходимо разработать некоторые рекомендации по совершенствованию механизма обеспечения информационной безопасности кредитной организации.

Технические средства защиты информации в банке, несомненно, являются самыми эффективными. Но помимо того, что компьютерная безопасность находится на должном уровне, следует также выделить несколько иных направлений в совершенствовании механизма обеспечения информационной безопасности в банке.[5]

На мой взгляд, одним из наиболее важных элементов является то, что в дежурной части банка должна быть подготовлена и заранее передана службе безопасности минимальная фиксированная информация, которая может быть

использована при включении сигнала тревоги (адрес банка, номера телефонов). Эта информация выдается на контрольный пункт автоматически вместе с получением сигнала тревоги. [8]Это, во-первых.

Во-вторых, необходимо совершенствование внутриобъектового режима, предусматривающего следующие основные требования[8]:

- строгое соблюдение сотрудниками правил экономической и информационной безопасности, правил противопожарной и противоаварийной безопасности и техники безопасности;

- установление порядка приема представителей сторонних организаций и работы с ними;

- определение порядка сдачи и приема помещений под охрану;

- установление порядка ведения телефонных, факсовых и телекоммуникационных обменов информацией с соблюдением режима конфиденциальности.

Система регулирования доступа в банке должна предусматривать:

- объективное определение надежности лиц, допускаемых к работе;

- максимальное ограничение количества лиц, допускаемых на объекты;

- установление для каждого работника дифференцированного по времени, месту и виду деятельности права доступа;

- четкое определение порядка выдачи разрешений и оформления документов для входа в банк;

- оборудование контрольно-пропускных пунктов техническими средствами, обеспечивающими достоверный контроль проходящих, объективную регистрацию прохода и предотвращение несанкционированного (в том числе силового) проникновения посторонних лиц.

Важнейшей составной частью общей системы безопасности банка является система организации контролируемого доступа сотрудников и клиентов банка в конкретные зоны и помещения. Она необходима для нейтрализации таких возможных угроз, как проникновение с целью грабежа, захвата заложников, отключение системы сигнализации, ликвидация персонала охраны, кражи коммерческой информации, установка подслушивающих устройств.

Для обеспечения пропускного режима для большей эффективности можно использовать методы идентификации личности. Например, различные пропуски (пропуск с фотографией, заменяемый пропуск с фотографией, пропуск с вызовом видеозаписи фотографии, закодированный пропуск); системы подтверждения характеристик (геометрические характеристики руки, отпечаток пальца, речевые характеристики и голос, рисунок сетчатки глаза, динамические характеристики почерка).

В-четвертых, необходимо совершенствование надежности персонала.[8] Данная политика может базироваться на разумном отборе персонала с помощью современных методов; продуманной и грамотно построенной системе вознаграждения и служебного роста; организационной культуре, поддерживающей в банке климат взаимоотношений; создании атмосферы сознательного отношения к безопасности, т.е. культуры безопасности.

Исходя из вышеперечисленного следует сказать, что банковская деятельность не стоит на месте, а это значит, что механизм обеспечения информационной безопасности должен совершенствоваться с учетом появления новых операций. Без правильно обеспеченной информационной политики ни один банк не сможет эффективно функционировать.

Библиографический список

1) Концепция информационной безопасности банка АККСБ «КС БАНК».

2) Белоглазова Г.Н. Банковское дело / Г.Н. Белоглазова, Л.П. Королевицкая. – М.: Финансы и статистика, 2011. – с. 115.

3) Букин С.О. Безопасность банковской деятельности / С.О. Букин. – М.:Питер, 2010. – с.25

4) Гамза В.А. Безопасность банковской деятельности / В.А. Гамза, И.Б. Ткачук. – М.: Маркет ДС, 2009. – с. 76.

5) Гафнер В.В. Информационная безопасность: Учебное пособие / В.В. Гафнер. - Рн/Д: Феникс, 2010. – с. 187.

6) Кормишкина Л.А. Экономическая безопасность предприятия (организации) / Л.А. Кормишкина, Е.Д. Кормишкин. – Саранск: Изд-во Мордов. ун-та, 2007. –с.67.

7) Партыка Т.Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. - М.: Форум, 2012. – с. 432.

8) Петров С.В. Информационная безопасность: Учебное пособие / С.В. Петров, И.П. Слинькова, В.В. Гафнер. - М.: АРТА, 2012. – с. 75.