Ермоленко Е. А.

УДК 33.07.336.719

Магистр 1 года обучения
факультета учет и аудит ХНЭУ им. С. Кузнеца

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БАНКОВСКИХ УЧРЕЖДЕНИЙ

Аннотация. Рассмотрена сущность информационной безопасности, определены проблемы информационной безопасности банковского учреждения и направления их решения. Рассмотрены понятия информационной безопасности банка. Определены основные меры и средства защиты информационной безопасности банковского учреждения.

Анотація. Розглянуто сутність інформаційної безпеки, визначено проблеми інформаційної безпеки банківської установи та напрями їх вирішення. Розглянуто поняття інформаційної безпеки банку. Визначено основні заходи і засоби захисту інформаційної безпеки банківської установи.

Annotation. The essence of information security has been studied, information security problems of a banking institution and solutions to them have been identified. The concepts of information security of a bank have been discussed. The main measures and remedies for information security of a banking institution have been identified.

Ключевые слова: информационная безопасность банка, информационные ресурсы банковского учреждения, угроза, защита.

Проблема безопасности информационных технологий сегодня приобретает особенную актуальность, что обусловлено, с одной стороны, стремительным развитием информационных технологий, с другой, имеет место значительное отставание теории и практики обеспечения безопасности по сравнению с динамикой технологическую прогресса [1]. Создание глобальной информационной среды обусловило возможности доступа к информационным ресурсам значительного количества пользователей различной квалификации, большинство из которых не имеют навыков обеспечения безопасности компьютерных систем на должном уровне.

Актуальность рассматриваемой проблемы обусловлена рядом взаимосвязанных факторов, большинство из которых является последствием процесса информатизации современного общества. Среди таких факторов, с одной стороны, − формирование правовых мероприятий информатизации, распространение применения современных информационных технологий, а с другой стороны – высокая уязвимость информационных систем.

В научных кругах тема информационной безопасности в банковских учреждений находится в центре постоянного внимания, что подтверждается работами таких авторов, как: Артеменко Д. А., Болгар Т. М., Адаменко С. И, Герасимов П. А., Шевцова О. И. [1 − 5].

Целью написания данной статьи является систематизация проблемы обеспечения информационной безопасности банковских учреждений и пути их решения.

Под информационной безопасностью банка понимается состояние защищенности информации о владельцах, руководства, клиентов банка, технологий и информационных ресурсов банка от внутренних и внешних угроз. Обеспечение информационной безопасности является неотъемлемой составляющей частью деятельности банка. Состояние информационной безопасности банка представляет собой умение и способность банка противостоять любым попыткам нанести ущерб законным интересам банка.

Структуру информационной безопасности банковских учреждений составляют:

безопасность информационных ресурсов;

безопасность информационной инфраструктуры;

безопасность "информационного поля" предприятия.

Информационные ресурсы банковского учреждения – это взаимосвязанная, упорядоченная, систематизированная и закрепленная на материальных носителях информация, которая принадлежит банковскому учреждению. Соответственно безопасность информационных ресурсов заключается в сохранении такой информации от несанкционированного распространения, использования и нарушения ее конфиденциальности [2].

Безопасность информационной инфраструктуры заключается в таком состоянии защищенности электронно-вычислительных машин (компьютеров), систем и компьютерных сетей, сетей электросвязи банковских учреждений, которая обеспечивает целостность и доступность информации, которая в них обрабатывается. Безопасность "информационного поля" банковского учреждения состоит в основном с несистематизированных потоков информации, обнародуется различными участниками информационных отношений: телерадиоорганизациями, печатными СМИ, Интернет-изданиями, конкурентами, органами государственной власти, местного самоуправления. Наиболее существенными угрозами безопасности информационных ресурсов является утечка или потеря таких ресурсов (в частности сведений, составляющих банковскую тайну).

Наиболее существенными угрозами безопасности информационных ресурсов является утечка или потеря таких ресурсов (в частности сведений, составляющих банковскую тайну). Угрозы информационным ресурсам могут быть реализованы путем [3]:

подкупа лиц, имеющих непосредственный доступ к банковской тайне и другой информации с ограниченным

доступом банковского учреждения;

неосторожного, небрежного обращения с банковской тайной и другой информации с ограниченным доступом;

несоблюдение требований сохранения информации с ограниченным доступом, установленных в учреждении, при контактах с контролирующими и наблюдательными органами в результате правовой и психологической неподготовленности ответственных работников банковского учреждения и т. п.

Для защиты информации банковских учреждений используют различные меры и средства защиты. Меры противодействия несанкционированному сбору информации в банке направляются на:

разработка соответствующей нормативной базы, которая регулирует режим и порядок доступа, хранения и использования информации банка;

контроль соблюдения мер информационной безопасности работниками банка;

защита информации в средствах и сетях ее передачи и обработки.

Защита информации банка с ограниченным доступом осуществляется всем персоналом банка в соответствии со служебными обязанностями. Разработка нормативной базы защиты информации в банке и контроль соблюдения информационной безопасности работниками банка осуществляет подразделение безопасности. Меры защиты информации в средствах и сетях ее передачи и обработки предусматривают использование аппаратных, программных и криптографических средствах защиты [4].

Аппаратные средства защиты применяются для решения таких заданий:

препятствия визуальному наблюдению и дистанционному подслушиванию;

нейтрализация паразитных электромагнитных излучений и наводок;

выявление технических средств подслушивания и магнитной записи, несанкционированно используемых в помещениях банка;

защита информации, передаваемой средствами связи и содержащаяся в системах автоматизированной обработки данных.

Программные средства защиты представляют собой специальные программы, включенные в программное обеспечение компьютеров и информационных систем, реализующих функции защиты конфиденциальной информации от неправомерных действий − несанкционированного доступа, копирования или разрушения. Проблемы обеспечения информационной безопасности банка и пути их решения представлены в таблице [5].

Таблица

Проблемы обеспечения информационной безопасности банка

Проблемы в обеспечении информационной безопасности банка	Причины возникновения	Средства и пути решения
1	2	3
Несанкционированный доступ	Нарушение должностных полномочий сотрудника, доступ к закрытой для публичного доступа информации со стороны лиц, не имеющих разрешения на доступ к этой информации	Защита информации от несанкционированного доступа осуществляется с помощью: • идентификации объектов и субъектов; • разграничению доступа к информационным ресурсам; • контроля и регистрации действий с информацией и программами

Окончание таблицы

1	2	3
Копирование	Копирование информации, как правило, представленной в электронном виде	Защита информации от копирования обеспечивается выполнением таких функций: • идентификация среды, из которой запускается программа копирования; • аутентификация среды, с которой запущена программа копирования; • реакция на запуск с несанкционированной среды; • регистрация санкционированного копирования; • противодействие изучению алгоритмов работы системы
Разрушение		Меры защиты от разрушения информации предусматривают: • запрет использования в банке несанкционированного программного обеспечения; • использования специальных антивирусных программ; • выполнение архивации и резервирования информации

Таким образом, обеспечение информационной безопасности банка − это система мер по обеспечению необходимого уровня информированности руководства и персонала банка, а также внешней среды, эффективная защита всех видов информации от внешних и внутренних угроз, которая достигается организацией сбора информации о внутренней и внешней среде банка, проведением информационно-аналитического исследования клиентов, партнеров и конкурентов, информационного аудита и информационного мониторинга в банке, аналитической обработкой информации; организацией системы информационного обеспечения принятия решений руководством банка; определением категорий банковской информации и выработкой соответствующих

мер ее защиты; соблюдением соответствующих режимов деятельности банка; выполнением всеми работниками банка норм и правил работы с информацией; своевременным выявлением проб и возможных каналов утечки информации и их нейтрализации.

Научн. рук. Мишин А. Ю.

Литература: 1. Артеменко Д. А. Механизм обеспечения финансовой безопасности банковской деятельности: дис. канд. экон. наук / Д. А. Артеменко. – 2005. 2. Болгар Т. М. Проблемы финансовой безопасности отечественных банков в условиях рыночной трансформации экономики / Т. М. Болгар // Академический обзор. – Днепропетровск : ДУЕП, 2007. − № 1. – С. 51−55. 3. Адаменко С. И. Характеристика и классификация угроз в банковской системе Украины / С. И. Адаменко // Стратегическая панорама. – 2004. − № 4. – С. 48−52. 4. Герасимов П. А. Экономическая безопасность банка : концептуальный подход / П. А. Герасимов // Банковские услуги. – 2006. − № 4. – С. 20−30. 5. Шевцова О. И. Современные аспекты банковской безопасности / О. И. Шевцова // Экономика: проблемы теории и практики : сб. научн. раб. : в 4 т. – Днепропетровск : Наука и образование, 2005. – Вып. 209. – Т. 2. – С. 546−554.