УДК 336.719.2

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СИСТЕМЕ БЕЗОПАСНОСТИ БАНКА

Гулько А. А.

кандидат экономических наук, доцент, доцент кафедры финансов, инвестиций и инноваций,

Белгородский государственный национальный исследовательский университет, Россия, Белгород

Антонян М. Г.

студентка кафедры финансов, инвестиций и инноваций,

Белгородский государственный национальный исследовательский университет, Россия, Белгород

Гордеева Ю.С.

студентка кафедры финансов, инвестиций и инноваций,

Белгородский государственный национальный исследовательский университет, Россия, Белгород

Аннотация

В статье исследуется понятие информационной безопасности и рассматривается ее сущность для банковской системы. Выявлены общие характеристики систем безопасности кредитных организаций. Предложены пути повышения безопасности отечественных банков с учетом нарастающих вызовов на финансовых рынках.

Ключевые слова: информационная безопасность, банковская безопасность, банковская система, банк, риски, угроза, кибератака.

INFORMATION SECURITY IN THE BANK SECURITY SYSTEM

Gulko A. A.

Candidate of Economic Sciences, Associate Professor, Assistant Professor of the Chair of Finance, Investments and Innovations,

Belgorod State National Research University,

Russia, Belgorod

Antonyan M. G.

student of the Department of Finance, Investments and Innovations,

Belgorod State National Research University,

Russia, Belgorod

Gordeeva Yu. S.

student of the Department of Finance, Investments and Innovations,

Belgorod State National Research University,

Russia, Belgorod

Annotation

The article explores the concept of information security and examines its essence for the banking system. The general characteristics of the security systems of credit institutions are revealed. The ways of increasing the safety of domestic banks are proposed, taking into account the growing challenges in the financial markets.

Keywords: information security, banking security, banking system, bank, risks, threat, cyberattack.

В условиях развития финансовых технологий и усиливающейся экономической нестабильности всё чаще встаёт вопрос о безопасности банка. Банковская система выступает неотъемлемой составляющей экономики и является необходимым условием национальной безопасности. Главная цель обеспечения банковской безопасности заключается, прежде всего, в обеспечении стабильного и эффективного функционирования кредитных организаций [4].

Стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» определяет безопасность, как состояние защищенности интересов (целей) организации бюджетной системы России в условиях угроз [1]. Именно своевременное выявление как внешних, так и внутренних угроз является

фундаментом для построения эффективного управления процессом обеспечения безопасности банковской деятельности.

Под безопасностью банковской деятельности понимают комплекс условий, позволяющий предупредить потенциально опасные для банка действия или обстоятельства, либо их свести к такому уровню, при котором они не способны причинить ущерб установленной системе функционирования банка, сохранению и воспроизводству его собственности и инфраструктуры, и затруднять достижение банком уставных целей [3].

В век компьютеризации всех сфер жизни общества и перехода к возможностям совершения многих банковских операций через сети Интернет стремительно возрастает и доля угроз, направленных на получение различного рода информации. Особенностями информационных систем банка является хранение ими огромного количества информации о финансовом положении физических и юридических лиц, а также их невозможность быть полностью закрытыми при использовании различных онлайн-систем. Применение данных банковских электронных систем делает защиту информации одной из главных проблем.

Статьями 8, 35, 114 Конституции РФ предусмотрено, что уголовно-правовое и административное пресечения противоправных действий в банковской сфере должно обеспечивать именно государство. Но, несмотря на это, большинство исследователей склоняются к тому, что главным субъектом обеспечения защиты российских банков от противоправных действий является государство, которое и должно выступать инициатором исследований в области банковской безопасности. Данное мнение неоднозначно. Банки должны самостоятельно осуществлять работу по организации системы предупреждения криминальных посягательств разного рода. В связи с этим, требования и рекомендации по принятию банками мер защиты своего имущества, содержащиеся в федеральных законах и нормативных актах Банка России, следует считать вполне оправданными. Именно банк должен своими силами и средствами обеспечивать безопасность своих активов, защиту

информационных ресурсов и информационной инфраструктуры, охрану имущества, физическую безопасность руководства и персонала и др. [3].

В рамках банковских платежных технологических процессов Центральный банк в качестве активов, требующих защиты в первую очередь, выделяет:

– банковский платежный технологический процесс;

– платежную информацию;

– информацию, отнесенную к защищаемой информации.

Информационная безопасность – это безопасность, связанная с угрозами в информационной сфере [1]. Основная цель информационной безопасности банка заключается в обеспечении эффективной деятельности банка путём исключения возможности нанесения ему ущерба. Как было сказано выше, источниками угроз выступают как внешние и внутренние нарушители, так и нарушения в работе программных и аппаратных компонентов информационных систем, а также природные и техногенные катастрофы. Выявление этих угроз, анализ возможных каналов и средств их реализации позволяют выработать рекомендации по обеспечению безопасности банков и банковских технологий, как на теоретическом, так и на практическом уровнях [2].

В области защиты информации банка главными задачами выступают:

– разработка нормативно-правовой базы и организация деятельности федеральных органов государственной власти и управления, органов государственной власти и управления субъектов РФ, местного самоуправления, организаций и предприятий для решения задач обеспечения государственной тайны, конфиденциальности информации и документов;

– установление баланса между потребностью в свободном обмене документами (сведениями) и допустимыми ограничениями доступа к ним;

– совершенствование информационной сферы, ускорение развития новых информационных технологий, их повсеместное применение, стандартизация средств поиска, сбора, обработки, хранения и анализа информации.

Для обеспечения их решения система информационной безопасности в банке должна иметь следующие характеристики:

– комплексный подход к защите системы, т.е. защищать все её компоненты;

– надежность в основе применения различных технологий кластеризации, балансировки нагрузки и др.;

– высокопроизводительность (обработка больших объемов информации без снижения быстродействия системы);

– быстрое и адекватное реагирование на различные инциденты, связанные с безопасностью [5].

Механизмы банковской защиты информации подразумевают защиту от утечек; контроль доступа; межсетевые экраны; антивирусы; программы шифрования информации и системы распознавания.

От уровня обеспечения безопасности автоматизированных информационных систем зависят конкурентоспособность и репутация банка, поскольку высокий уровень безопасности снижает следующие риски: риск распространения информации, угрожающей банку; риск потери важных данных; риск утечки конфиденциальной, тайной информации.

К общим принципам осуществления обеспечения информационной безопасности банков относят:

– своевременное установление, обнаружение и устранение проблем;

– возможность прогнозирования развития;

– анализ актуальности и эффективности предпринятых мер.

В целях обеспечения эффективной системы управления информационной безопасностью банки должны:

– выявлять и оценивать риски по всем, в том числе новым, продуктам и системам банка;

– осуществлять сбор данных и убытков от реализации рисков;

– разрабатывать и реализовывать мероприятия, направленные на снижение вероятности рисков и минимизацию последствий от их реализации;

– осуществлять регулярный мониторинг уровня рисков и др. [7].

Таким образом, процесс управления безопасностью должен включать следующие основные этапы:

– выявление риска, т.е. определение предпосылок, причин и обстоятельств реализации риска;

– оценку риска – банк анализирует информацию, полученную в результате идентификации риска, определяет вероятность наступления событий риска, приводящих к потерям, а также размера ущерба;

– анализ проблемных зон процессов банка, выработка и принятие решения по оптимизации процессов для снижения уровня риска;

– мониторинг риска;

– контроль выполнения мероприятий по снижению уровня риска и устранению проблемных зон в процессах [6].

Несмотря на общие принципы обеспечения информационной безопасности банков, каждая кредитная организация вырабатывает свою политику безопасности.

Следует отметить, что, в связи с политической обстановкой в мире, все чаще нарастают угрозы кибератак; несанкционированного доступа к информации банковских систем; перехват, искажение информации, передаваемой по каналам связи и др.

Всем банкам необходимо выполнять требования к кибербезопасности, определенные в нормативных документах Банка России. Следует тщательно отбирать персонал, имеющий доступ к информации; иметь программы защиты от атаки вирусов и надежное специализированное программное обеспечение; применять межсетевые экраны и др.

Для защиты банковской безопасности необходима постоянная разработка и обновление программных продуктов и электронных систем. Важным моментом в разработке программного обеспечения является анализ угроз. Анализ позволяет улучшить осведомленность руководства и сотрудников, ответственных за безопасность системы, об её сильных и слабых сторонах, и,

тем самым, способствует созданию базы для принятия верных решений и оптимизации системы безопасности для более эффективной работы. Правильно выбранная политика информационной безопасности позволит отечественным банкам снизить риски утечки конфиденциальной информации и, как следствие, повысить эффективность их деятельности.

Библиографический список:

1. Стандарт Банка России: «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» (СТО БР ИББС-1.0-2014) [Электронный ресурс] // Центральный банк Российской Федерации. Режим доступа: http://www.cbr.ru/credit/Gubzi_docs/main.asp?Prtid=Stnd, свободный.
2. Атаманов, Г. А. О банковской безопасности и безопасности банков [Текст] / Г. А. Атаманов // право и безопасность . – 2013. – № 1-2. – С. 79–85.
3. Гамза, В. А. Безопасность банковской деятельности : учебник для вузов [Текст] / В. А. Гамза, И. Б. Ткачук, И. М. Жилкин. – 3-е изд., перерад. и доп. – М.: Издательство Юрайт, 2015. – 513 с.
4. Гулько, А. А. К вопросу об обеспечении информационной безопасности коммерческих банков [Текст] / А. А. Гулько, Гладкова С. Б., Битюкова А. Ф. [и др.] // Экономика и предпринимательство. – 2016. – № 3-1. – С. 588–592.
5. Мовсесян, Е. Л. Информационная безопасность в банковских системах [Текст] / Е. Л. Мовсесян, М. В. Перова // Перспективы развития информационных технологий. – 2014. – № 21. – С. 145–150.
6. Годовой отчет 2016 [Электронный ресурс] // Сбербанк. – Режим доступа: http://www.sberbank.com/ru/investor-relations/reports-and-publications/annual-reports, свободный.
7. Меры безопасности [Электронный ресурс] // РоссельхозБанк. – Режим доступа: http://www.rshb.ru/security/, свободный.