ISSN 2311-8768 (Online)
ISSN 2073-4484 (Print)

Мониторинг и прогнозирование банковских рисков

СОВЕРШЕНСТВОВАНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЭЛЕКТРОННЫХ РАСЧЕТОВ В КОММЕРЧЕСКИХ БАНКАХ РОССИИ

Ольга Михайловна МАРКОВА

кандидат экономических наук, доцент кафедры банков и банковского менеджмента,
Финансовый университет при Правительстве РФ, Москва, Российская Федерация
markova1310@bk.ru

История статьи:
Принята 02.07.2015
Одобрена 13.07.2015

УДК 336.075.8

Ключевые слова: система управления, информационная безопасность, электронные расчеты, автоматизация, банковская система

Аннотация

Предмет. В связи с совершенствованием требований к информационной безопасности банковских операций рассматриваются важные изменения в области законодательного регулирования электронных расчетов и новые модели управления системами безопасности, которые позволяют снизить риски возможных потерь при осуществлении электронных расчетов.

Цели и задачи. Цель работы — показать изменения в области законодательного регулирования электронных расчетов в свете применения стандарта Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения (СТО БР ИББС-1.0-2014)» и разработанных рекомендаций в области стандартизации РС БР ИББС-2.6-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Обеспечение информационной безопасности на стадиях жизненного цикла автоматизированных банковских систем». Раскрыть направления совершенствования управления безопасностью электронных расчетов на основе систем управления качеством безопасности расчетов, что позволит повысить степень защищенности кредитной организации в сфере информационных технологий и сделает более стабильным банковский бизнес.

Методология. В работе проанализированы различные аспекты информационной безопасности банковской деятельности, определены наиболее эффективные системы управления информационной деятельностью в коммерческих банках.

Результаты. Приведены предложения, направленные на совершенствование информационной безопасности и средств ее защиты в коммерческих банках, которые связаны с определением информационных и технических ресурсов, подлежащих защите, выявлением потенциально возможных угроз и каналов утечки информации, проведением оценки уязвимости и рисков информации при имеющемся множестве угроз и каналов утечки, определением требований к системе защиты, выбором средств защиты информации и их характеристик, внедрением и организацией использования выбранных мер, способов и средств защиты, осуществлением контроля за целостностью системы защиты информации.

Вывод. В условиях усиления экономических санкций значительно повышаются требования к обеспечению информационной безопасности электронных расчетов, что позволяет повысить надежность банковского бизнеса в России.

Обеспечение информационной безопасности электронных расчетов в коммерческих банках — это системный процесс, который требует разработки комплекса мер, направленных на снижение уровня потерь до минимального (приемлемого) уровня и который позволяет снизить вероятность его наступления в будущем. В связи с увеличением внешних и внутренних угроз при обработке платежной и иной информации усиливаются риски банковской деятельности, что в свою очередь значительно увеличивает уязвимость информационной безопасности банковской деятельности [1, 2].

В рамках преобразования национальной платежной системы России в Банке России и коммерческих банках значительно повышаются требования к участникам электронных расчетов в области информационной безопасности[1]. Поэтому возникает

[1] Федеральный закон от 27.06.2011 № 161-ФЗ «О национальной платежной системе»; положение Банка России от 29.06.2012 № 384-П «О платежной системе Банка России».

необходимость обеспечения качественно нового уровня развития систем защиты информационной безопасности [3]. Для коммерческих банков и Банка России очень важными становятся задачи по разработке концепции безопасности в области осуществления электронных расчетов, по выявлению и изучению разных видов рисков информационной безопасности, а также механизму их раннего выявления и предотвращения.

Указанные требования были обусловлены изменениями законодательства России в области информационной безопасности (в частности, документами Федерального агентства по техническому регулированию и метрологии, Технического комитета по стандартизации «Стандарты финансовых операций», подкомитета по стандартизации «Безопасность финансовых (банковских) операций», поправками в Федеральный закон от 27.12.2002 № 184-ФЗ «О техническом регулировании»).

На этом основании Банк России с 01.06.2014 ввел в действие ряд новых документов, касающихся стандартизации информационной безопасности, в том числе:

– новую (пятую) редакцию стандарта Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения (СТО БР ИББС-1.0-2014)»;
– четвертую редакцию стандарта Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации» (далее — СТО БР ИББС-1.0-2014)[2].

Одновременно с этими документами Банком России была доработана «Методика оценки соответствия информационной безопасности коммерческих банков требованиям СТО БР ИББС-1.0-2014», а также были разработаны новые рекомендации по стандартизации информационной безопасности, в том числе РС БР ИББС — 2.5-2014 (менеджмент инцидентов информационной безопасности)[3] [3, 4].

Таким образом, Банк России постоянно совершенствует систему мер по регулированию безопасности информационных систем, которая направлена на продвижение инвестиционных и инновационных проектов на отечественных и зарубежных рынках, а также на развитие банковского сектора и повышение его стабильности и надежности. Особенно это актуально в условиях усиления экономических санкций и внешнего давления на банковскую систему России [5].

Рассмотрим более подробно новые положения СТО БР ИББС-1.0-2014 и его существенные отличия от версии 2010 г. [6].

В новом документе были представлены более точные определения понятий «банковский платежный технологический процесс» и «банковский информационный технологический процесс» (пп. 3.28 и 3.29 СТО БР ИББС-1.0-2014), раскрыты возможные нарушения информационной безопасности (инцидент информационной безопасности), которые обусловливаются недостатками действующих средств защиты информации (п. 3.48. СТО БР ИББС-1.0-2014).

В стандарте было введено понятие «самооценка информационной безопасности» и уточнено понятие «аудит информационной безопасности» (пп. 3.64, 3.65 СТО БР ИББС-1.0-2014). Были разработаны новые исходные концептуальные схемы (парадигма) обеспечения информационной безопасности банковской системы Российской Федерации. В частности, к ней относится необходимость недопущения ее нарушения, вызванного повышением операционных рисков банковской системы. Для этого предлагается введение единой карты рисков при оценке стоимости ущерба в целом для кредитной организации (п. 5.15 СТО БР ИББС-1.0-2014).

Важные изменения коснулись также анализа возможных моделей угроз и выявления нарушителей информационной безопасности кредитных организаций. Было принято целесообразным устанавливать процедуры регулярного анализа этих угроз и выявления конкретных сотрудников банка, ответственных за нарушения информационной безопасности (п. 6.12 СТО БР ИББС-1.0-2014). Исходя из этого, коммерческим банкам запрещается осуществлять электронное обслуживание клиентов, если не был обеспечен соответствующий уровень квалификации работников в сфере электронных расчетов.

[2] Стандарт Банка России СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации» от 06.01.2014.

[3] Рекомендации в области стандартизации Банка России РС БР ИББС-2.5-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Менеджмент инцидентов информационной безопасности» (приняты и введены в действие распоряжением Банка России от 17.05.2014 № Р-400).

В качестве актива для защиты информационной безопасности был введен дополнительный объект — информация, отнесенная к защищаемой информации в соответствии с п. 2.1 Положения Банка России от 09.06.2012 № 382-П (п. 7.1.9 СТО БР ИББС-1.0-2014)[4]. Было предложено внедрить в банковскую практику принцип предоставления минимальных прав и полномочий, необходимых для выполнения своих обязанностей (служебных), а также ответственность сотрудников банков за обеспечение информационной безопасности банковских систем (помимо должностных инструкций). Также внесены соответствующие изменения в организационно-распорядительные документы кредитных организаций (пп. 7.2.1 и 7.2.2 СТО БР ИББС-1.0-2014).

Значительно повышены требования к обеспечению информационной безопасности в заданиях по разработке и доработке автоматизированной банковской системы, а также по анализу принятия разработчиком автоматизированной банковской системы защитных мер, которые направлены на выполнение мероприятий по обеспечению безопасности разработки автоматизированной банковской системы (пп. 7.3.4, 7.3.6 СТО БР ИББС-1.0-2014).

Кроме того, изменениям были подвергнуты требования по выполнению контроля, связанного с уменьшением уязвимости оборудования и программного обеспечения автоматизированной банковской системы к угрозам в части информационной безопасности, параметров настройки автоматизированной банковской системы, а также применяемых защитных мер (технических), обновления программного обеспечения автоматизированной банковской системы (п. 7.3.9 СТО БР ИББС-1.0-2014).

В частности, были рассмотрены вопросы о необходимости выполнения и учета процедур контроля за составом устанавливаемого (используемого) программного обеспечения автоматизированной банковской системы, определения и назначения ролей, которые связаны с контролем и эксплуатацией автоматизированной банковской системы [7] и которые необходимы для обеспечения сохранности носителей (машинных) защищаемой информации (пп. 7.3.11–7.3.13 СТО БР ИББС-1.0-2014). Это позволило в процессе функционирования или доработки автоматизированных банковских систем, которые отнесены к критичным, увеличить требования по определению, регистрации и выполнению процедур учета внесенных изменений и проверки функциональности автоматизированных банковских систем после внесения изменений (п. 7.3.15 СТО БР ИББС-1.0-2014).

Кроме того, были четко определены процедуры и алгоритмы удаления информации по причине морального износа, а также амортизации автоматизированных банковских систем (п. 7.3.16 СТО БР ИББС-1.0-2014). Значительные изменения претерпел также раздел общих требований в области обеспечения безопасности информации при доступе и регистрации пользователей.

В организации банковской системы РФ должны быть определены, выполняться, регистрироваться и контролироваться правила и процедуры:

- идентификации, аутентификации, авторизации субъектов доступа,
- разграничения доступа к информационным активам;
- управления учетными записями субъектов доступа;
- управления идентификационными и аутентификационными данными и средствами;
- использования мобильных устройств;
- управления предоставлением и/или прекращением доступа;
- использования технологий беспроводного доступа информации;
- регистрации действий субъектов доступа, выявления и блокирования попыток несанкционированного доступа;
- блокирования сеанса доступа после установленного времени бездействия или по запросу субъекта доступа, требующего выполнения процедур повторной аутентификации (п. 7.4.3 СТО БР ИББС-1.0-2014).

Также был детально проработан вопрос об определении, выполнении, регистрации и контроля правил и процедур мониторинга информационной безопасности. Определены требования о введении журналов по контролю за операциями автоматизированных рабочих мест, межсетевых

[4] Положение Банка России от 09.06.2012 № 382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств».

экранов, автоматизированных банковских систем, работой серверного и сетевого оборудования в коммерческих банках, а также рекомендации о хранении этих журналов с информацией о действиях и операциях работников в течение трех или более лет, а в случае сбора информации в платежных технологиях — пяти лет или более (с учетом законодательства России) (п. 7.4.4 СТО БР ИББС-1.0-2014).

Коснулись изменения и порядка доступа работников в помещения расположения информационных систем, которые регулируют информационное взаимодействие между сегментами вычислительных сетей, межсетевое экранирование, разделение сегментов вычислительных сетей.

В отдельный пункт был выделен порядок доступа работников в помещения, согласно которому требуется осуществлять регистрацию и контроль за доступом работников организации к объектам области информационных активов (пп. 7.4.5, 7.4.6 СТО БР ИББС-1.0-2014). Появилось требование о необходимости регламентации использования съемных носителей.

Важными направлениями стандартизации информационной безопасности являются необходимость сетевого протоколирования участков линий связи и телекоммуникационных каналов (в том числе и беспроводных), а также требование об обеспечении защиты от раскрытия и модификации защищаемой информации по каналам связи (пп. 7.4.14, 7.4.15 СТО БР ИББС-1.0-2014). При этом большое значение отводится антивирусной проверке перед подключением съемных носителей информации на специально выделенном автономном средстве вычислительной техники. Для этого были введены ограничения по передаче с использованием сети Интернет защищаемых данных только при условии обеспечения защиты информации от раскрытия и модификации (п. 7.6.2 СТО БР ИББС-1.0-2014).

Предлагается ввести в действие инструкции и рекомендации по использованию сети Интернет, учитывающих особенности организации, а также требования по определению и выполнению процедур протоколирования использования ресурсов сети Интернет работниками организации (п. 7.6.4 СТО БР ИББС-1.0-2014).

Повышению безопасности информационных систем и банковского платежного технологического процесса будет способствовать требование о блокировке приема к исполнению распоряжений клиентов. Для этого предлагается усилить защиту информационной безопасности на устройствах, задействованных в осуществлении электронных расчетов (пункт 7.8.10 СТО БР ИББС-1.0-2014).

Существенное нововведение — это требование о необходимости определения, контроля и выполнения мероприятий по обеспечению информационной безопасности в процессе взаимодействия автоматизированных банковских систем кредитных организаций с информационными системами сторонних организаций (п. 7.9.5 СТО БР ИББС-1.0-2014).

Кардинально переработаны разделы общих требований по обработке персональных данных в кредитной организации, а также общих требований информационной безопасности технологических процессов, которые обрабатывают персональные данные клиентов банка, с учетом современных требований и изменений законодательства РФ (п. 7.10 СТО БР ИББС-1.0-2014).

Значительно повышен уровень требований в области управления информационной безопасностью кредитных организаций путем внесения в соответствующий раздел минимальных полномочий службы информационной безопасности требований о необходимости ее контроля на всех стадиях жизненного цикла автоматизированных банковских систем, а также вменено как обязательство руководству кредитной организации осуществление самооценки информационной безопасности.

Таким образом, Банк России в рамках масштабных реформ разработал новые документы по развитию платежных услуг и обеспечению информационной безопасности расчетов. В частности, в формулы оценки показателей информационной безопасности были введены корректирующие коэффициенты, которые позволяют точнее осуществлять оценку ее обеспечения [4].

Однако следует отметить, что СТО БР ИББС-1.2-2014 применяется на добровольной основе, тогда как требования Положения Банка России № 382-П[5] являются обязательными. Подобное разночтение законодательных и рекомендательных положений, к которым относится рассматриваемый стандарт,

[5] Положение Банка России от 09.06.2012 № 382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств».

Рисунок 1

Система управления информационной безопасностью коммерческого банка

обусловлено тем обстоятельством, что он дает более гибкие возможности оценки информационной безопасности. Его использование совместно с Положением Банка России № 382-П позволит существенно повысить степень защищенности кредитной организации в сфере информационных технологий и сделать более стабильным банковский бизнес [4].

Разработанные рекомендации Банка России «Менеджмент инцидентов информационной безопасности» (РС БР ИББС-2.5-2014) позволяют выстраивать процессы управления инцидентами с меньшими операционными рисками и финансовыми затратами.

Помимо законодательных требований в области информационной безопасности коммерческие банки должны внедрять в практику новые модели управления системами безопасности, которые позволяют снизить риски возможных потерь при осуществлении электронных расчетов[6] [8]. Структура системы управления информационной безопасностью (СУИБ) коммерческого банка приведена на рис. 1.

При управлении информационной безопасностью электронных расчетов актуальной является модель Деминга [9], в которую включены элементы управления качеством результатов деятельности банка (организации): «планирование — выполнение — проверка — действие» (рис. 2).

В этой модели элементы управления результатом деятельности банка учитываются через:

- планирование, как определение процессов и целей, необходимых для получения результатов, согласно миссии банка и его политике информационной безопасности;
- выполнение (реализацию), как результат выполнения запланированных решений и процессов;
- проверку на основе измерения и контроля процессов и производимых результатов деятельности по отношению к политике информационной безопасности, требований и целей по отношению к результатам деятельности банка;
- действие (совершенствование), как учет в деятельности корректирующих мер для совершенствования процесса.

Эта схема по отношению к системе управления информационной безопасностью представлена на рис. 3.

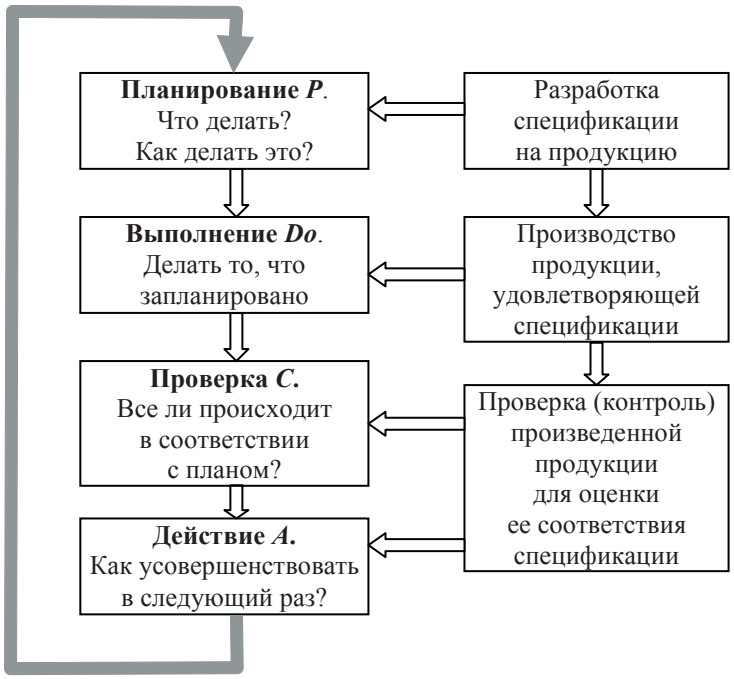
Анализ рис. 3 позволяет сделать вывод, что фактически защиту информации в коммерческом банке можно свести к следующим последовательным мерам, с обязательной обратной связью:

- *во-первых,* провести организационные меры защиты информации (порядок обеспечения информационной безопасности);

[6] *Трещалин С., Семенов Р.* Информационная безопасность в зоне риска. URL: http://nbj.ru/publs/upgrade-modernizatsija-i-razvitie/2015/05/05/informatsionnaja-bezopasnost-v-zone-riska/index.html.

Рисунок 2

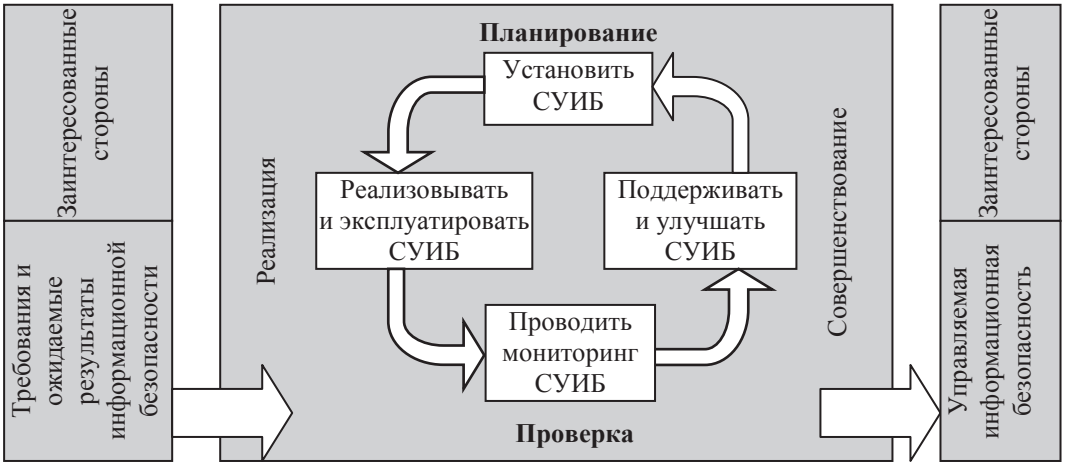
Управление качеством результата деятельности банка (модель Деминга)



Источник: [9].

Рисунок 3

Управление качеством работы системы управления информационной безопасности (модель Деминга)



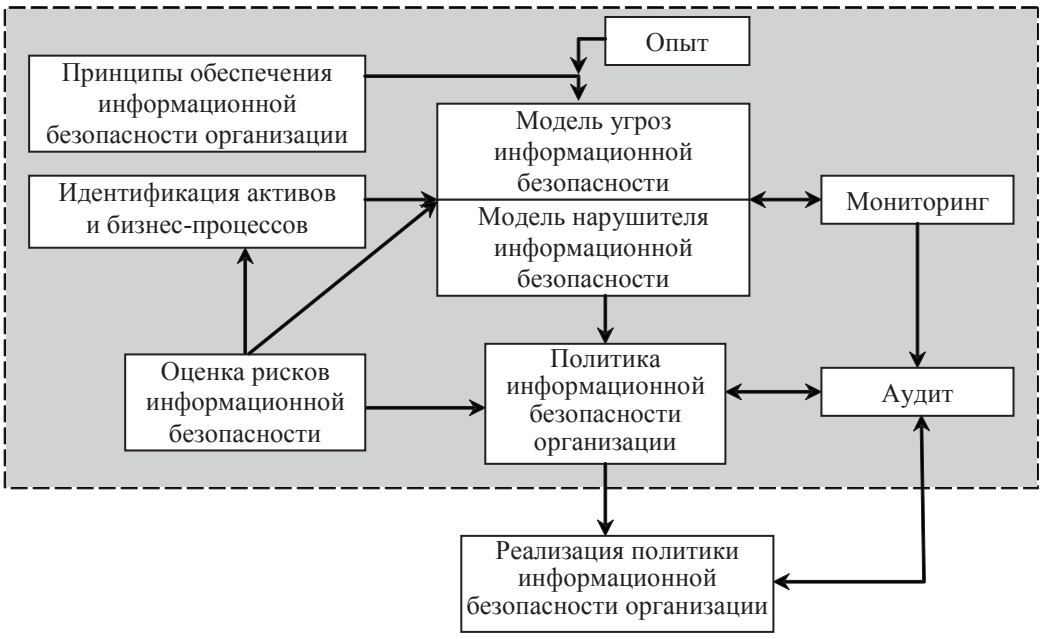
– *во-вторых,* применять способы защиты информации (в том числе и технической);
– *в-третьих,* осуществлять постоянный мониторинг обеспечения защиты информации через внутренний и внешний контроль;
– *в-четвертых,* требуется эволюция IT-систем для оценки ее влияния на банковский бизнес [10].

В рамках рассмотренной модели системы управления информационной безопасностью электронных расчетов можно выявить способы реализации модели, к которым следует отнести:

– принципы обеспечения информационной безопасности;
– идентификацию активов и бизнес-процессов, связанных с информационной безопасностью;
– оценку рисков различных моделей;
– необходимость разработки политики риск-менеджмента коммерческого банка в области

Рисунок 4

Способы реализации модели управления информационной безопасностью в коммерческом банке



информационной безопасности с обязательным мониторингом и аудитом защитных мер (рис. 4) [11, 12].

В модели управления информационной безопасностью в коммерческом банке необходимо учитывать, что наиболее эффективным способом измерения уровня информационной безопасности является управление безопасностью в рамках нескольких составляющих, а именно:

- в области управления рисками;
- в области управления инцидентами;
- в области проверки и оценки деятельности по обеспечению информационной безопасности.

Следует рассмотреть риски наступления неблагоприятных событий по косвенным признакам, в частности путем измерения соответствующих показателей, которые характеризуют состояние информационной безопасности банка [13].

Для этого в коммерческом банке необходимо разработать политику предотвращения рисков информационной безопасности и выявления соответствующих угроз, приводящих к уязвимости его активов [14] (рис. 5).

Риск — это когда уязвимость соответствует угрозе, что наглядно проиллюстрировано на рис. 6.

Следует учитывать, что в случае полной или частичной реализации угрозы рисков информационной безопасности это приводит, как правило, к инцидентам. Под инцидентом информационной безопасности понимается возникновение одного или нескольких нежелательных событий информационной безопасности, которые могут с большой долей вероятности скомпрометировать операции в деятельности коммерческих банков и Банка России [4].

Событие информационной безопасности — это появление определенного состояния актива (сети, сервиса, системы) коммерческих банков и Банка России (идентифицированное), которое может привести к нарушению в области политики информационной безопасности или средств защиты, либо может возникнуть неизвестная ситуация, имеющая отношение к информационной

Рисунок 5

Воздействие возникшей угрозы на информационную безопасность

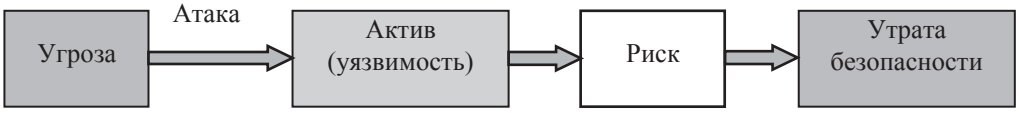
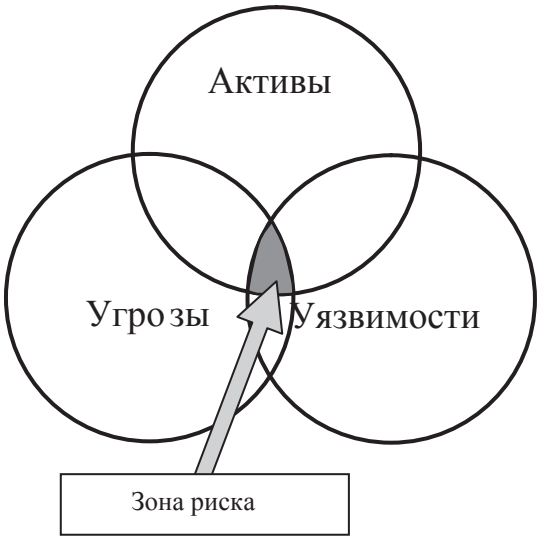


Рисунок 6

Взаимодействие «угроза — актив — уязвимость»



Источник: [14]

безопасности. Возникающими инцидентами нужно уметь грамотно управлять и выявлять основные тенденции в управлении качеством электронных банковских услуг [15] (рис. 7).

Управление инцидентами информационной безопасности включает управление процессами, где на входе отражается информация, которая получена при сборе и протоколировании событий информационной безопасности, а на выходе — информация, по причине которой произошел инцидент информационной безопасности, и показаны меры предотвращения инцидента информационной безопасности в будущем (рис. 8).

Обеспечение перечисленных условий является целью управления инцидентами информационной безопасности. Необходимо, чтобы все события информационной безопасности были своевременно обнаружены, быстро и качественно обработаны (несмотря на то, относятся или не относятся они к категории инцидентов информационной безопасности). Инциденты информационной безопасности, которые были идентифицированы, должны быть грамотно оценены. Реализация мер по их ликвидации (или снижению) должна быть адекватной и максимально результативной.

Защитные меры должны минимизировать отрицательные воздействия инцидентов информационной безопасности на деятельность банка. Свершившиеся инциденты информационной безопасности ложатся в основу опыта и используются для предотвращения инцидентов информационной безопасности, которые могли бы возникнуть в последующей деятельности банка и его бизнес-процессах [2].

Следовательно, усилия коммерческих банков по обеспечению информационной безопасности сводятся к мерам по предотвращению последствий неблагоприятных событий (оценки уровня безопасности, так называемого рискового подхода), который может быть реализован в рамках разработки соответствующей модели по управлению информационной безопасностью с учетом оценки стоимости информации для сокращения потерь и расширения возможностей бизнеса [16].

Таким образом, для поддержания эффективного уровня информационной безопасности необходимо учитывать:

– типы уязвимости в действующей конфигурации систем, которые могут быть использованы при осуществлении несанкционированного доступа;
– достаточность реализованных защитных мер для предотвращения существующих рисков информационной безопасности;

Рисунок 7

Управление инцидентами информационной безопасности

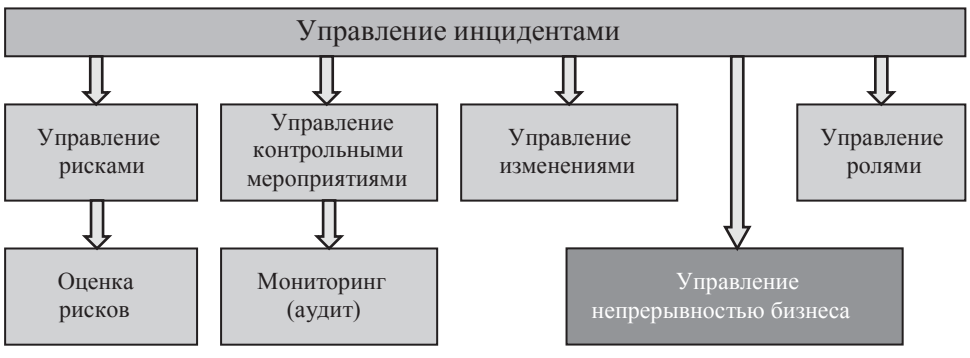
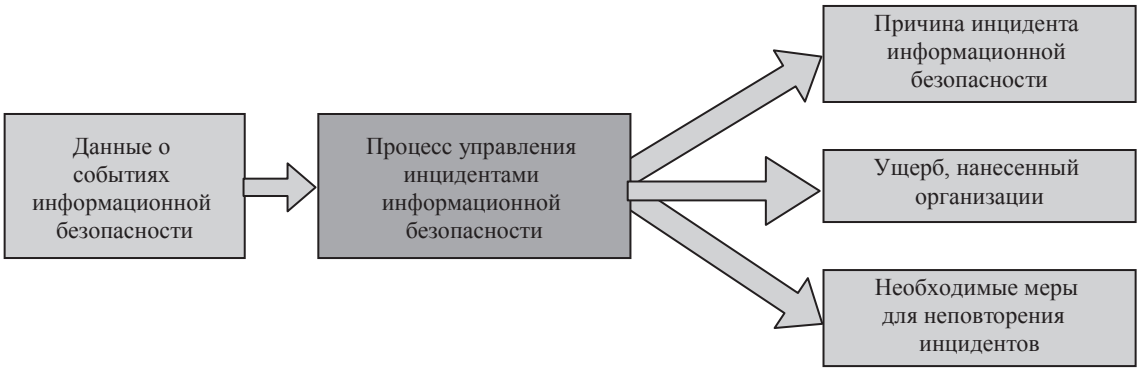


Рисунок 8

Меры предотвращения угрозы информационной безопасности



– эффективность защиты объекта в существующей среде функционирования;
– интеграцию информационных систем корпоративных клиентов и банка [17].

Поскольку защитные меры со временем ослабевают и работают уже не так эффективно, необходимо выявить критерии и действия по проверке и оценке управления информационной безопасностью. Кроме этого, используя процессный подход, следует дать оценку эффективности обеспечения информационной безопасности.

Оценка и проверка деятельности по обеспечению информационной безопасности — это элемент управления информационной безопасностью, который нужен для того, чтобы выявить признаки ухудшения используемых в организации защитных мер. Для этого необходимы:

– мониторинг информационной безопасности и контроль за используемыми защитными мерами;
– самооценка информационной безопасности (в пределах заданного интервала времени с программой и планом проведения);
– внутренний и внешний аудит функционирования системы управления информационной безопасности (с заданной периодичностью).

Следовательно, для эффективного предотвращения рисков и угроз информационной безопасности в операционной среде коммерческого банка необходим постоянный мониторинг информационной безопасности (контроль за защитными мерами), который позволяет проводить регулярное и непрерывное наблюдение за объектами и субъектами, несущими угрозу безопасности, а также осуществлять самооценку выполнения банком установленных критериев информационной безопасности.

Регулярный внутренний аудит информационной безопасности, проводимый сотрудниками ревизионных структур Банка России и коммерческих банков, усиливает контроль за функционированием разных аспектов обеспечения информационной безопасности и регламентируется их внутренними документами.

Для достижения большего эффекта контрольных мер и формирования аудиторского (профессионального) суждения о состоянии информационной безопасности в коммерческом банке необходим, помимо внутреннего аудита, также и внешний аудит информационной безопасности — протоколируемый процесс (систематический и независимый) получения свидетельств деятельности по обеспечению информационной безопасности коммерческих банков и Банка России, проводимый внешней независимой проверяющей организацией [18].

Таким образом, Банк России и коммерческие банки должны использовать эффективные механизмы предотвращения внешнего и внутреннего воздействия на информационные системы, информационные технологии и новые виды банковского сервиса, а также учитывать передовой опыт в области защиты банковских информационных активов.

Список литературы

1. *Гончаренко Л.П.* Управление безопасностью. М.: КноРус, 2013. 272 с.
2. *Йохан Балийон*. Современные тенденции в области информационной безопасности банков // Банковское дело. 2014. № 10. С. 60–63.

3. *Лахно Ю.В*. Инновационные решения в структуре национальной платежной системы // Банковское дело. 2014. № 8. С. 56–58.
4. *Сердюк В*. Роль стандартов Банка России в обеспечении информационной безопасности кредитно-финансовых организаций // Бухгалтерия и банки. 2008. № 3.
5. *Фролов Д., Неваленный А*. Противодействовать кризису. Особенности обеспечения информационной безопасности в кредитно-финансовой сфере в условиях кризиса // BIS Journal. Информационная безопасность банков. 2015. № 2.
6. *Марданов Р.Х., Ильин И.В*. Стандарты информационной безопасности в банковской системе // Вестник Уфимского государственного авиационного технического университета. 2013. Т. 17. № 7. С. 55–60.
7. *Сумманен К*. Автоматизация управления банковскими рисками // Connect. Мир информационных технологий. 2015. № 5.
8. *Астахов А*. Искусство управления информационными рисками. М.: ДМК Пресс, 2010. 314 с.
9. *Деминг В.Э*. Новая экономика для промышленности, правительства и образования. М.: Экономика, 2003. 328 с.
10. *Пущилин В*. Эволюция IT-систем — влияние на банковский бизнес // Банковские технологии. 2015. № 4.
11. *Варфоломеев А.А*. Основы информационной безопасности. М.: РУДН, 2008. 412 с.
12. *Филипенков Н*. Смогут ли банки выжить без современной системы риск-менеджмента // Банковское обозрение. 2014. № 11.
13. Банковские электронные услуги / под ред. О.С. Рудаковой. М.: Вузовский учебник, 2012. 400 с.
14. *Выборнов А*. Устранение уязвимостей // BIS Journal. Информационная безопасность банков. 2014. № 4.
15. *Никпур А., Донюк Х*. Основные тенденции в управлении качеством электронных банковских услуг // Банковское дело. 2015. № 3. С. 54–58.
16. *Хаббард Д.У*. Оценка стоимости информации: сокращение потерь и расширение возможностей. URL: http://www.elitarium.ru/2014/03/05/ocenka_stoimosti_informacii.html.
17. *Дубровский Ю.В*. Интеграция информационных систем корпоративных клиентов и банка // Банковское дело. 2015. № 1. С. 62–64.
18. *Просвирина Е.М*. Индикаторы экономической безопасности // Банковское дело. 2014. № 12. С. 76–81.

ISSN 2311-8768 (Online)
ISSN 2073-4484 (Print)

Monitoring and Prediction of Banking Risks

IMPROVING THE INFORMATION SECURITY OF ELECTRONIC PAYMENTS IN COMMERCIAL BANKS OF RUSSIA

Ol'ga M. MARKOVA

Financial University under Government of Russian Federation, Moscow, Russian Federation
markova1310@bk.ru

Article history:
Received 2 July 2015
Accepted 13 July 2015

Keywords: management system, information security, electronic payments, automation, banking system

Abstract

Importance Considering the changes in requirements to the information security of banking transactions, the research overviews important amendments to legislative regulation of electronic payments, and new models for managing security systems, which allow mitigating risks of possible losses when making electronic payments.

Objectives The research strives to reflect the changes in legislative regulation of electronic payments assuming that the Bank of Russia's standard *Ensuring the Information Security of Entities Operating in the Banking System of the Russian Federation* is applied. The article discloses areas for improving the electronic-payment security management systems on the basis of payment security quality management, thus increasing the security of the credit institution in terms of information technologies and making the banking business more sustainable.

Methods The research analyzes various aspects of information security in banking, and determines the most effective systems for managing the information security in banking.

Results I present my proposals for improving the information security and ways to keep it in commercial banks. For this, it is necessary to identify information and technological resources to be protected, potential threats and data leakage channels; assess susceptibility and risks of information considering threats and data leakage channels; determine requirements to the protection system; to choose data protection means and their characteristics; organize and enforce the measures, methods and means of protection; control the data protection system integrity.

Conclusions and Relevance I conclude that tightened economic sanctions considerably increase requirements to information security of electronic payments, thus making the banking business in Russia more reliable and safe.

References

1. Goncharenko L.P. *Upravlenie bezopasnost'yu* [Security management]. Moscow, KnoPus Publ., 2013, 272 p.
2. Balijon Johan. Sovremennye tendentsii v oblasti informatsionnoi bezopasnosti bankov [Modern trends in information security of banks]. *Bankovskoe delo = Banking*, 2014, no. 10, pp. 60–63.
3. Lakhno Yu.V. Innovatsionnye resheniya v strukture natsional'noi platezhnoi sistemy [Innovative solutions in the national payment system]. *Bankovskoe delo = Banking*, 2014, no. 8, pp. 56–58.
4. Serdyuk V. Rol' standartov Banka Rossii v obespechenii informatsionnoi bezopasnosti kreditno-finansovykh organizatsii [The role of standards of the Bank of Russia in ensuring the security of credit and financial institutions]. *Bukhgalteriya i banki = Accounting and Banks*, 2008, no. 3.
5. Frolov D., Nevalennyi A. Protivodeistvovat' krizisu. Osobennosti obespecheniya informatsionnoi bezopasnosti v kreditno-finansovoi sfere v usloviyakh krizisa [Countering the crisis. Specifics of ensuring the information security in the lending and financial sector during the crisis]. *BIS Journal. Informatsionnaya bezopasnost' bankov = BIS Journal. Information Security of Banks*, 2015, no. 2.
6. Mardanov R.Kh., Il'in I.V. Standarty informatsionnoi bezopasnosti v bankovskoi sisteme [Information security standards in the banking system]. *Vestnik Ufimskogo gosudarstvennogo aviatsionnogo tekhnicheskogo universiteta = Vestnik of Ufa State Aviation Technical University*, 2013, vol. 17, no. 7, pp. 55–60.
7. Summanen K. Avtomatizatsiya upravleniya bankovskimi riskami [Automation of banking risks management]. *Connect. Mir informatsionnykh tekhnologii = Connect. The World of Information Technologies*, 2015, no. 5.

8. Astakhov A. *Iskusstvo upravleniya informatsionnymi riskami* [The art of managing information risks]. Moscow, DMK Press Publ., 2010, 314 p.
9. Deming W.E. *Novaya ekonomika dlya promyshlennosti, pravitel'stva i obrazovaniya* [The New Economics for Industry, Government and Education]. Moscow, Ekonomika Publ., 2003, 328 p.
10. Pushchilin V. Evolyutsiya IT-sistem — vliyanie na bankovskii biznes [The evolution of IT systems is an impact on banking]. *Bankovskie tekhnologii= Banking Technologies*, 2015, no. 4.
11. Varfolomeev A.A. *Osnovy informatsionnoi bezopasnosti* [Fundamentals of information security]. Moscow, Peoples' Friendship University of Russia Publ., 2008, 412 p.
12. Filipenkov N. Smogut li banki vyzhit' bez sovremennoi sistemy risk-menedzhmenta [Will banks be able to survive without a modern risk management system?]. *Bankovskoe obozrenie = Banking Review*, 2014, no. 11.
13. *Bankovskie elektronnye uslugi* [Electronic banking services]. Moscow, Vuzovskii uchebnik Publ., 2012, 400 p.
14. Vybornov A. Ustranenie uyazvimostei [Fixing of vulnerabilities]. *BIS Journal. Informatsionnaya bezopasnost' bankov = BIS Journal. Information Security of Banks*, 2014, no. 4.
15. Nikpur A., Donyuk Kh. Osnovnye tendentsii v upravlenii kachestvom elektronnykh bankovskikh uslug [Major trends in quality management of electronic banking services]. *Bankovskoe delo = Banking*, 2015, no. 3, pp. 54–58.
16. Hubbard D.W. *Otsenka stoimosti informatsii: sokrashchenie poter' i rasshirenie vozmozhnostei* [Measuring the Value of Information. In: How to Measure Anything]. Available at: http://www.elitarium.ru/2014/03/05/ocenka_stoimosti_informacii.html. (In Russ.)
17. Dubrovskii Yu.V. Integratsiya informatsionnykh sistem korporativnykh klientov i banka [Integration of information systems of corporate clients and Bank]. *Bankovskoe delo = Banking*, 2015, no. 1, pp. 62–64.
18. Prosvirina E.M. Indikatory ekonomicheskoi bezopasnosti [Indicators of economic security]. *Bankovskoe delo = Banking*, 2014, no. 12, pp. 76–81.