Министерство внутренних дел Российской Федерации
Казанский юридический институт

Н.Р. Шевко
О.Г. Шмелева
Г.Н. Хадиуллина

ОБЕСПЕЧЕНИЕ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ В БАНКОВСКОЙ СФЕРЕ ПРИ ИСПОЛЬЗОВАНИИ ИНСТРУМЕНТОВ ЭЛЕКТРОННОГО БАНКИНГА

Монография

Казань 2017

ББК 32.81
Ш 31

Одобрено редакционно-издательским советом КЮИ МВД России

Рецензенты
Доктор экономических наук, профессор **А.М. Туфетулов**
(Казанский (Приволжский) федеральный университет)

Доктор экономических наук, доцент **Л.Ф. Нугуманова**
(КНИТУ им. А.Н. Туполева)

Шевко Н.Р.

Ш 31 Обеспечение экономической безопасности в банковской сфере при использовании инструментов электронного банкинга : монография / Н.Р. Шевко, О.Г. Шмелева, Г.Н. Хадиуллина. – Казань : КЮИ МВД России, 2017. – 89 с.

Монография содержит научное обоснование принципов, форм и методов обеспечения экономической безопасности финансовых операций при использовании средств электронного банкинга.

Предназначена для профессорско-преподавательского состава, слушателей и курсантов образовательных организаций системы МВД России.

ISBN 978-5-906977-08-3 **ББК 32.81**

© Шевко Н.Р., Шмелева О.Г., Хадиуллина Г.Н., 2017
© КЮИ МВД России, 2017

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Одним из необходимых элементов экономической системы современного государства выступает банковская система, от эффективности функционирования в значительной степени зависят состояние и направления развития национальной экономики в целом, отдельных субъектов хозяйствования, а также уровень и качество жизни населения. В свою очередь, изменение факторов внешней среды банковских организаций, включающих процессы глобализации экономического пространства, трансформацию нормативно-правовой базы, активное использование информационно-коммуникационных технологий и др., приводит к возникновению новых и усилению действующих угроз их функционирования. Тем самым в современном мире актуализируется проблема формирования действенной системы безопасности банковской деятельности. При этом система экономической безопасности банков становится объектом управления на микро- и макроуровнях, что обусловлено прямой зависимостью показателей функционирования экономики в целом и отдельных банковских организаций от эффективности инструментов управления рисками.

В рамках данного исследования безопасность банка (банковская безопасность) рассматривается как совокупность внешних и внутренних условий банковской деятельности, при которых потенциально опасные для банковской системы и отдельного банка действия (бездействия) или обстоятельства (риски и угрозы) предупреждены, пресечены либо сведены к такому уровню, при котором не способны нанести ущерб установленному порядку банковской деятельности (функционированию банка, сохранению и воспроизводству имущества и инфраструктуры банковской системы или отдельного банка) и воспрепятствовать достижению банком уставных целей. Надежность

обеспечения безопасности банка оценивается по степени уязвимости от рисков и угроз защищаемых элементов его имущества и инфраструктуры. В составе факторов внешней среды выделяются факторы прямого (клиенты, конкуренты на рынке банковских услуг, стейкхолдеры и др.) и косвенного воздействия (нормативная правовая база, порядок налогообложения, уровень развития информационно-коммуникационных технологий (ИКТ) и др.).

Для формирования действенной системы безопасности банковской деятельности представляется необходимым сформулировать принципы ее функционирования, определения состава и описания источников угроз, выявления инструментов управления рисками банковской деятельности, формирования механизмов противодействия легализации преступных доходов и финансирования терроризма в банковских учреждениях. Комплексный подход к оценке уровня безопасности банковской деятельности должен отвечать следующим требованиям: оценивать, с одной стороны, возможности противостоять банковским кризисам, а с другой - возможности развития, расширения деятельности; оценивать безопасность банковской системы, проецируя ее развитие на экономику территории размещения и национальной экономики в целом; проводить регулярный мониторинг состояния безопасности банковской деятельности на основании системы показателей; выявлять риски банковской деятельности и своевременно предпринимать меры, обеспечивающие их нейтрализацию.

Безопасности банковской деятельности посвящено значительное число работ, в которых безопасность банков рассматривается с разных точек зрения, в частности, безопасности банков, экономической безопасности, финансовой безопасности, безопасности проведения банковских операций и др. Однако следует признать необходимость дальнейших исследований в данной сфере, в которых наряду с концептуальными основами формирования безопасности банковской деятельности должны быть определены риски эффективного функционирования банковской системы, а также представлены конкретные рекомендации органам государственного управления и топ-менеджменту банковских организаций относительно состава мер по управлению рисками банковской деятельности.

При организации эффективной системы безопасности банковской деятельности необходимо придерживаться таких принципов, как комплексность, своевременность, законность, обоснованность, экономическая специализация, взаимодействие и координация, усовершенствование, централизация. Основной целью функционирования системы безопасности банков является предупреждение убытков от разглашения конфиденциальной информации; кражи финансовых и материально-технических ценностей, нарушения функционирования информационных систем. Указанная цель соответствует целевым ориентирам системы национальной безопасности государства, которые определены в Стратегии национальной безопасности и включают: укрепление обороны страны, обеспечение незыблемости конституционного строя, суверенитета, независимости, государственной и территориальной целостности Российской Федерации; укрепление национального согласия, политической и социальной стабильности, развитие демократических институтов, совершенствование механизмов взаимодействия государства и гражданского общества; повышение качества жизни, укрепление здоровья населения, обеспечение стабильного демографического развития страны; сохранение и развитие культуры, традиционных российских духовно-нравственных ценностей; повышение конкурентоспособности национальной экономики; закрепление за Российской Федерацией статуса одной из лидирующих мировых держав, деятельность которой направлена на поддержание стратегической стабильности и взаимовыгодных партнерских отношений в условиях полицентричного мира[1].

Заданиями системы безопасности банковской деятельности должны быть: своевременное выявление и ликвидация угроз, факторов и условий, которые вызывают финансовый, материальный и моральный убыток банковской системе; отнесение информации к категории ограниченного доступа; создание механизма и условий оперативного реагирования на угрозы безопасности и появление негативных тенденций в функционировании банковской системы; создание

[1] О Стратегии национальной безопасности Российской Федерации: указ Президента Российской Федерации от 31 декабря 2015 года № 683. URL: https://rg.ru/2015/12/31/nac-bezopasnost-site-dok.html (дата обращения: 20.07.2017).

условий для максимально возможного возмещения и локализации убытков, которые получены на основании неправомерных действий физических и юридических лиц, для послабления негативного влияния нарушений безопасности на достижение стратегических целей.

Общая схема организации безопасности банковской деятельности содержит действия (мероприятия), которые осуществляются последовательно или одновременно, а именно: формирование необходимого ресурсного потенциала (капитала, персонала, прав, информации, технологии и оборудования); общестратегическое прогнозирование и планирование финансовой безопасности за функциональными составляющими; стратегическое прогнозирование для обеспечения финансовой устойчивости банковской системы; общетактическое планирование безопасности банковской деятельности за функциональными составляющими; тактическое прогнозирование в системе обеспечения финансовой устойчивости банковской системы; осуществление функционального анализа уровня безопасности банковской деятельности; общая оценка достигнутого уровня безопасности банковской деятельности.

Целью написания данной монографии выступает обоснование основных компонентов, которые определяют концептуальные основы системы безопасности банковской деятельности, что определило состав задач исследования: определить экономическую сущность безопасности банковской деятельности; охарактеризовать основные элементы безопасности банковской деятельности; обосновать основные угрозы, которые влияют на уровень безопасности банковской деятельности; установить взаимосвязь между уровнем безопасности банковской деятельности и финансовой устойчивостью банковской системы; сформулировать рекомендации относительно содержания локального нормативного акта - Политики коммерческого банка в сфере информационной безопасности.

Представленная монография рассчитана на банковских работников, работников подразделений УЭБ и ПК МВД по Республике Татарстан, а также может быть использована в учебном процессе КЮИ МВД России и других образовательных организаций системы МВД России.

Глава 1.
ПОНЯТИЕ, ПРИНЦИПЫ И СПОСОБЫ ОБЕСПЕЧЕНИЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ БАНКОВ

1.1. Сущность экономической безопасности банков и ее место в системе национальной безопасности

Способность государства эффективно противостоять влиянию имеющихся либо потенциальных угроз его существованию и независимому развитию составляет содержание национальной безопасности. В составе национальной безопасности отдельно выделяют такие ее составляющие, как:

1) военная безопасность;
2) политическая безопасность;
3) социокультурная безопасность;
4) экологическая безопасность;
5) экономическая безопасность.

Экономическая безопасность является главной составляющей национальной безопасности и трактуется как качественная характеристика экономической системы, которая определяет ее способность поддерживать нормальные условия работоспособности системы, развитие в рамках целей, поставленных перед ней, а в случаях возникновения различных угроз (внешних и внутренних) – способность системы противостоять им и восстанавливать свою работоспособность.

Выделяют несколько уровней экономической безопасности:

1) международная безопасность (глобальная, региональная);
2) национальная безопасность – государства, отрасли, региона, общества;

3) частная безопасность – предприятия, домашнего хозяйства или личности.

Финансовая безопасность является подсистемой экономической безопасности государства. Финансовая безопасность государства - это такое состояние финансовой, денежно-кредитной, валютной, банковской, бюджетной и налоговой систем, которое характеризуется сбалансированностью, устойчивостью к внутренним и внешним негативным влияниям, способностью обеспечить эффективное функционирование национальной экономической системы и ее рост.

Банковская система является важнейшей составляющей финансово-кредитной сферы государства. Именно состояние банковского сектора и определяет уровень финансово-кредитной безопасности, а, следовательно, во многом и уровень финансовой безопасности государства.

Понятие экономической безопасности банковской системы, как правило, определяется как состояние, при котором финансовая стабильность и репутация банковских учреждений не могут быть утрачены из-за целенаправленных действий определенной группы лиц или организации как внутри, так и за границами государства, а также из-за негативных макроэкономических и политических факторов. Таким образом, экономическая безопасность банка - это состояние, при котором обеспечиваются экономическое развитие и стабильность деятельности банка, гарантированную защиту его финансовых и материальных ресурсов, способность адекватно и без существенных потерь реагировать на изменения внутренней и внешней ситуации.

Безопасность как система основана на противодействии существующим угрозам. Она характеризует состояние объекта в целом и обеспечивается для защиты от:

1. Нарушения нормального хода воспроизводительного процесса.
2. Преступного мира.
3. Нарушений закона (чтобы самим не попасть под санкции).
4. Недобросовестной конкуренции.
5. Некомпетентных и противоправных действий собственных сотрудников.

Угрозы финансовым ресурсам банка проявляются в виде: невозврата кредитных ссуд; мошенничества со счетами и вкладами; под-

ложных платежных документов и пластиковых карт; хищения финансовых средств из касс и инкассаторских машин; резкого изменения экономической ситуации в стране (экономические кризисы); банкротства деловых партнеров банка.

Угрозы информационным ресурсам проявляются в виде: разглашения коммерческой тайны; утечки конфиденциальной информации через технические средства обеспечения производственной деятельности различного характера и исполнения; несанкционированного доступа к охраняемым сведениям со стороны конкурентных организаций и преступных формирований; уничтожения или порчи носителей стратегически важной информации вследствие злонамеренных действий или несчастных случаев; ведения "информационной войны" против банка, наносящий существенный ущерб его деловой репутации.

Проблемы банковской сферы являются одновременно и проблемами финансовой безопасности государства. Стабильность и надежность банковской системы, усовершенствование банковского менеджмента и укрепление его стратегической составляющей могут обеспечить финансовую безопасность государства. В целом можно констатировать, что проблемам обеспечения финансовой безопасности банковских учреждений посвящено достаточно небольшое количество исследований. Этим, в частности, объясняется отсутствие единого общепринятого подхода к определению данного понятия. Также нужно отметить, что довольно большое количество авторов вообще игнорируют вопросы финансовой безопасности и, как правило, рассматривают либо экономическую безопасность банка, либо безопасность вообще.

Деятельность по обеспечению безопасности хозяйствующего субъекта осуществляется, как правило, по следующим направлениям:

1. Производственное (сохранность материальных ценностей, контроль над соблюдением технологий, поиск и использование резервов повышения эффективности).

2. Кадровое обеспечение (подбор и расстановка кадров, повышение профессионализма, продвижение кадров, контроль над лояльностью и преданностью компании, системы поощрения, мотивация труда).

3. Коммерческое (анализ рынка, продвижение продукции, прогноз деятельности, оценка партнеров).

4. Финансово-экономическое (анализ деятельности, выработка целей, разработка прогноза и планов, оценка финансового положения, кредитная и инвестиционная политика, оценка рисков, создание резервов).

5. Юридическое (оценка нормативно-правовой базы, подготовка договоров и контроль над их исполнением, юридическое сопровождение и защита).

6. Информационное (определение значимости информации, порядок поступления информации, защита от хищения и проникновения в сети).

7. Собственная безопасность (концепция безопасности, разработка системы безопасности, разведка и контрразведка, охрана, защита, контроль над деятельностью).

Безопасность банковской системы необходимо рассматривать в двух аспектах:

1) с точки зрения финансовых последствий деятельности банков для страны в целом и отдельных клиентов и контрагентов;

2) с точки зрения недопущения и предотвращения явных и потенциальных угроз финансовому состоянию всей банковской системы страны, Центрального Банка РФ и отдельных банковских учреждений.

Задача методического обеспечения банковской безопасности актуальна в двух плоскостях. Во-первых, ее решение позволяет сохранить финансовую стабильность конкретного банка, а во-вторых, решение задачи на более высоком государственном уровне призвано обезопасить экономику страны, сократить количество финансовых махинаций и уменьшить влияние теневого сектора экономики. Наряду с решением системных задач по управлению деятельностью банка возникает необходимость в разрешении ряда специфических вопросов, посвященных защите интересов банка от различного рода противозаконных посягательств путем выполнения функций обеспечения банковской безопасности.

В более узком смысле обеспечение банковской безопасности можно рассматривать как системную деятельность по предотвраще-

нию или снижению тяжести последствий противоправных действий, затрагивающих интересы банка.

Поскольку кредитно-финансовые операции являются основным источником дохода современного банка, основная угроза банковской безопасности непосредственно вызвана противоправными действиями, совершаемыми в плоскости кредитно-финансовой деятельности.

В современных условиях развития информационных технологий большую опасность для банка представляют так называемые интеллектуальные мошенники, которые используют в своей деятельности достижения современных технологий. Поэтому на данном этапе развития современного общества следует отождествлять термин "банковская безопасность", прежде всего, именно с защитой от интеллектуальных атак. Таким образом, наряду с задачами по обеспечению основной кредитно-финансовой деятельности возникают особые задачи по защите интересов банка путем выполнения функций обеспечения банковской безопасности, направленных на упреждение или снижение тяжести последствий противоправных действий, которые нежелательны для банка.

Безопасность отдельного банка тесно связана с безопасностью банковской системы в целом. Они оказывают влияние друг на друга. С одной стороны, проблемы, возникшие в одном банке, способны вызвать «эффект домино» и привести к системному банковскому кризису, что объясняется самой природой банковской деятельности. С другой стороны, структурные проблемы банковского сектора подрывают доверие к любому отдельно взятому банку. Все это объясняет ту важную роль, которую играет обеспечение финансовой безопасности банков.

Таким образом, под экономической безопасностью банка в широком смысле следует понимать обеспечение наиболее эффективного использования всех ресурсов банка для предотвращения угроз и создания условий стабильного функционирования всех его подразделений. При этом к источникам угроз относятся нежелательные изменения финансовой конъюнктуры на рынках, технологические инновации, форс-мажорные обстоятельства.

Исходя из различных трактовок сущности безопасности в банковской деятельности, проанализированных нами выше, можем выделить следующие ключевые характеристики безопасности банков:

1. Обеспечивает равновесное и устойчивое финансово-экономическое состояние банка.

2. Способствует эффективной деятельности банка; позволяет на ранних стадиях определить проблемные места в деятельности банка.

3. Нейтрализует кризисы и предупреждает банкротство.

При этом для обеспечения безопасности банка необходимо решить такие задачи, как:

1. Обеспечение достаточной финансовой устойчивости и независимости банка.

2. Поддержание технологической независимости и конкурентоспособности, формирование высокого технического и технологического потенциала.

3. Оптимизация организационной структуры, постоянное усовершенствование выполнения функций менеджмента.

4. Правовая защита всех видов деятельности банка.

5. Создание защиты информационной среды банка, его коммерческой тайны.

6. Формирование условий для безопасной работы сотрудников банка.

7. Сохранение и эффективное использование финансовых, материальных и информационных ресурсов банка.

Основная цель безопасности банка состоит в непрерывном и устойчивом поддержании такого состояния, которое характеризуется сбалансированностью и устойчивостью к влиянию внешних и внутренних угроз.

Перед службами безопасности банков стоят следующие задачи:

1) идентификация рисков и связанных с ними потенциальных опасностей и угроз;

2) определение индикаторов безопасности банка;

3) внедрение системы диагностики и мониторинга состояния безопасности;

4) разработка мероприятий, направленных на обеспечение безопасности банка как в краткосрочном, так и в долгосрочном периоде;

5) контроль выполнения запланированных мероприятий;

6) анализ выполнения мероприятий, их оценка, корректировка;

7) идентификация опасностей и угроз банку и корректировка индикаторов в зависимости от изменения состояния внешней среды, целей и задач банка;

8) участие в уголовном и административном преследовании виновных в посягательстве на интересы банка в соответствии с законодательством РФ.

Функции службы безопасности банка:

• участвовать в плановых и внеплановых проверках деятельности подразделений банка методами оперативного, административного и финансового контроля;

• проводить внутренние (служебные) расследования по фактам причинения ущерба интересам банка;

• готовить материалы к направлению в правоохранительные органы для решения вопроса о возбуждении уголовного дела в соответствии с УПК РФ;

• собирать и представлять следственным органам документы (в том числе материалы фото- и киносъемки, аудио- и видеозаписи и иные носители информации) и предметы для приобщения их к уголовному делу в качестве доказательств;

• использовать в этих целях средства и методы криминалистики.

Основные направления деятельности службы безопасности банка включают:

• защиту от преступлений, посягающих на собственность банка: хищения денежных средств при совершении кредитных и расчетно-кассовых операций; мошенничество в сфере корпоративного и потребительского кредитования; хищения денежных средств с использованием платежных поручений, требований, чеков, векселей и аккредитивов;

• защиту от преступлений, посягающих на порядок функционирования банка: злоупотребление полномочиями, коммерческий подкуп, посягательства на сведения банка, составляющие банковскую, коммерческую и иную тайну, посягательства в сфере компьютерного обеспечения деятельности банка, посягательства на кадровое обеспечение банка, посягательства на нематериальные активы банка;

• организацию противодействия отмыванию преступных доходов и финансированию терроризма.

Организационные методы включают в себя специальные методы осуществления управленческой, финансовой, коммерческой, кадровой и иной функциональной деятельности банка, имеющие целью предупредить причинение ущерба как в результате умышленных и неосторожных противоправных действий, так и вследствие ошибки. В рамках этих методов формируются специальные подразделения контроля и защиты интересов банка; проводится совершенствование структуры банка; принимаются решения об ограничении полномочий должностных лиц в отношении объема и состава банковских операций, в распоряжении денежными средствами и иным имуществом банка; определяются полномочия по осуществлению расчетно-кассовых операций и пассивно-активных операций; устанавливается ответственность за обеспечение процедур выполнения отдельных операций и порядка хранения ценностей; организуется система контроля, отчетности и работы с персоналом.

Функциональные методы обеспечения безопасности банка включают:

1. Технологические методы (технологические решения, закрепленные распорядительными документами) основываются на рекомендациях Банка России, разработках подразделений банка, рекомендациях экспертов.

2. Методы обеспечения конфиденциальности информации: закрытие свободного доступа к информации, отнесенной к охраняемой законом тайне; защита информации в каналах связи и средствах вычислительной техники; предупреждение и пресечение попыток неправомерного завладения сведениями и документами.

3. Методы административного контроля: проверка правильного функционирования системы подбора и расстановки кадров, наличия и исполнения должностных инструкций сотрудников.

4. Методы финансового контроля обеспечивают проведение операций в строгом соответствии с принятой и закрепленной документами политикой банка применительно к разным видам финансовых операций и услуг и их адекватного отражения в учете и отчетности.

Криминалистические методы обеспечения безопасности банка включают:

1. Технико-криминалистические средства, которые используются для предупреждения преступлений и административных правонарушений. Их применение: а) затрудняет или исключает возможность совершения посягательства; б) создает благоприятные условия для формирования и сбора доказательственной информации.

2. Приемы криминалистической тактики, которые используются для построения и контроля функционирования системы безопасности банка. Применяются: построение версий о видах и характере потенциальных угроз и способах защиты от них; планирование мероприятий по выявлению причин и условий, способствующих совершению посягательств; «следственный» эксперимент по проверке надежности мер защиты интересов банка; экспертное исследование материалов.

3. Рекомендации криминалистической методики используются для создания методик предотвращения, пресечения и внутреннего расследования отдельных видов противоправных посягательств.

Криминалистическая характеристика противоправного посягательства – это система описания присущих тому или иному виду посягательства особенностей, позволяющих обеспечить эффективное предупреждение, пресечение и расследование этих посягательств и обусловливающих применение соответствующих методов, приемов и средств.

Элементы криминалистической характеристики:

– предмет противоправного посягательства;

– типичные способы совершения и сокрытия посягательства;

– обстоятельства подготовки и совершения посягательства (время, место, условия, участники и т.п.);

– характерные механизмы следообразования;

– типология личности виновного и потерпевшего.

Основу эффективности деятельности по информационному обеспечению безопасности банка составляет процесс поиска, получения, накопления, анализа и использования необходимой информации. Качество информационного процесса является основным критерием оценки профессионализма службы безопасности банка и ее отдельных работников. Добываемая информация должна быть четко «привя-

зана» к конкретным объектам защиты и предполагаемым видам противоправных посягательств, обеспечивать возможность применения на ее основе норм правовой защиты и соответствовать установленным законодательством условиям ее собирания и использования. В современных условиях эффективными являются специальные аналитические технологии для предупреждения и расследования противоправных посягательств на безопасность банка, использующие широкий спектр баз данных, включая Интернет.

Правовые аспекты безопасности банка включают процесс реализации законодательства, регламентирующего полномочия, обязанности и ответственность органов государственной власти, Банка России, представительных и исполнительных органов банка, связанные с обеспечением его безопасного функционирования. Правовую основу банковской безопасности составляют: федеральные законы, нормативные правовые акты Президента РФ, Правительства РФ, субъектов федерации, ведомственные нормативные акты; нормативные акты Банка России в форме указаний, положений и инструкций, а также его рекомендации и официальные разъяснения по вопросам применения федеральных законов и иных нормативных правовых актов; локальные нормативные акты банка.

Локальные нормативные акты банка в сфере безопасности включают:

1. Акты общего характера, регламентирующие технологию осуществления банковских операций, распределяющие функции и полномочия между подразделениями и сотрудниками банка, определяющие процедуру принятия решений, регулирующие деятельность службы внутреннего контроля и службы безопасности.

2. Акты по вопросам обеспечения безопасности: объектовый режим безопасности банка; режим защиты сведений ограниченного доступа (перечень информации, составляющей коммерческую (банковскую) тайну, положение об организации защиты информации ограниченного доступа и компьютерной информации, инструкция о распределении доступа пользователей к информации ограниченного доступа, к осуществлению операций в автоматизированной банковской системе, а также к базам данных в компьютерных системах); по-

рядок организации и функционирования службы безопасности (положение о службе безопасности, инструкция о проведении внутренних расследований по фактам нарушений порядка обеспечения безопасности банка).

Таким образом, безопасность банка является важной составляющей национальной безопасности и представляет собой такое состояние банковского учреждения, которое характеризуется сбалансированностью и устойчивостью к влиянию внешних и внутренних угроз, его способностью достигать поставленные цели и генерировать достаточный объем финансовых ресурсов для обеспечения устойчивого развития. Недостаточное внимание обеспечению безопасности банков может привести к проблемам в деятельности финансовых учреждений.

1.2. Основные направления деятельности подразделений банковской безопасности

Реализация риска ведет к ущербу для результатов деятельности банка, поэтому, как правило, в его организационной структуре создается служба (управление) банковской безопасности (ББ). Чаще всего целью деятельности службы (подразделений) банковской безопасности является защита интересов банка от ошибок, злоупотреблений и преступлений со стороны персонала, клиентов, конкурентов и других лиц и организаций.

При своевременном выявлении источников каждое событие отмеченных и других рисков переходит в разряд конкретной угрозы, имеющей установленный источник и содержание. Функции службы (подразделений) банковской безопасности заключаются в снижении или ликвидации отмеченных рисков, и (или) в своевременном выявлении рисков, переводе их в разряд конкретных угроз и последующем упреждении реализации таких угроз, а в случае реализации угрозы - в снижении тяжести ее последствий для деятельности банка.

В связи с этим деятельность подразделения банковской безопасности реализуется по следующим основным направлениям:

1. Своевременное выявление реальной и (или) потенциальной угрозы жизненно важным интересам банка, его работникам и акционерам со стороны банков-конкурентов.

2. Установление внутренних и внешних причин и условий, которые способствуют нанесению материального ущерба банку, его работникам, акционерам и клиентам, препятствуют нормальному функционированию и развитию банка.

3. Разработка и реализация механизма оперативного реагирования на угрозы и негативные тенденции, которые возникают по отношению к банку.

4. Предупреждение посягательств на законные интересы банка, его работников, акционеров и клиентов, использование юридических, технических, организационных и иных способов для выявления и ликвидации источников угроз его безопасности.

5. Локализация и максимально полное возмещение убытков банка, полученных в результате неправомерных действий со стороны физических и юридических лиц.

6. Уменьшение вредных последствий от акций банков - конкурентов и (или) уголовных элементов в результате непосредственного подрыва безопасности банка и создания неблагоприятных условий для его деятельности в достижении поставленных целей.

7. Создание благоприятных условий для реализации банком своих основных интересов.

Отмеченную совокупность основных направлений деятельности служба банковской безопасности выполняет в рамках следующих функций:

1. Административно-распорядительной, которая реализуется путем разработки, внедрения и поддержки в банке, в его структурных подразделениях и филиалах режима безопасности.

2. Учетно-контрольной, которая обеспечивается путем организации своевременного выявления реальной и потенциальной угрозы финансовой стабильности, устойчивости деятельности банка по реализации своих основных интересов, путем оценки и контроля источников этой угрозы.

3. Социально-кадровой, которая реализуется путем участия

управления ББ в подборе, проверке и расстановке кадров; выявлении отрицательных тенденций в коллективах структурных подразделений банка и его филиалах, возможных причин и условий возникновения социального напряжения; предупреждении и локализации возможных конфликтов.

4. Организационно-управленческой, которая реализуется путем организационного, материально-технического и технологического обеспечения режимов безопасности банка и его филиалов.

5. Методической функции, которая реализуется путем выявления, накопления и внедрения в деятельность банка положительного опыта по вопросам обеспечения безопасности.

6. Информационно-аналитической, которая реализуется путем целенаправленного сбора, накопления, обработки и предоставления информации, актуальной для сферы обеспечения безопасности управления банком, путем организации аналитической обработки такой информации с использованием всех накопленных в банке данных.

Для достижения успеха деятельности по отмеченным направлениям организация службы банковской безопасности в банке должна удовлетворять следующим известным требованиям: непрерывности, устойчивости, активности, прогнозирования и предупреждения нарушений, комплексности и плановости. При этом участие специалистов банковской безопасности предусматривается во всех основных сферах деятельности банка. Каждая сфера деятельности является многогранной и включает значительное количество мероприятий банковской безопасности, требующих своевременных действий. Такие мероприятия преследуют выполнение задач, которые формируются в группы близких по области реализации и способам выполнения.

Состав задач, близких по направлениям решения и способам действий специалистов подразделений банковской безопасности, является определяющим для формирования организационной структуры подразделений банковской безопасности и включает следующие элементы:

1. Обеспечение экономической безопасности.
2. Ликвидация проблемной задолженности.
3. Финансовый мониторинг.
4. Защита технологии платежных карточек.

5. Кадровая работа.
6. Техническая защита информации.
7. Охрана служебных помещений, ценностей и должностных лиц.

Выполнение задач банками Российской Федерации сопряжено с разделением и специализацией труда банковских работников. Такая специализация, с одной стороны, позволяет повышать квалификационный уровень работников и добиваться заметных успехов в профессиональной деятельности, а с другой - создает благоприятные условия для злоупотреблений в банковской сфере, для действий, противоречащих законным интересам банков. Для защиты интересов банка от ошибок, злоупотреблений и преступлений со стороны персонала, клиентов и третьих лиц, организаций в банке создается служба банковской безопасности.

В соответствии с существующими научно-методическими подходами к обеспечению банковской безопасности и с целью решения отмеченных задач, как правило, в головном офисе банка организуется управление банковской безопасности, а в областных филиалах - отдел банковской безопасности. Кроме того, в крупных балансовых отделениях для выполнения необходимого объема работ могут назначаться отдельные работники банковской безопасности. Управление банковской безопасности, как правило, является самостоятельным структурным подразделением банка и в соответствии с группами, близкими по направлениям решения задач, имеет в своем составе следующие отделы:

1. Отдел экономической безопасности.
2. Отдел работы с проблемной задолженностью.
3. Отдел финансового мониторинга.
4. Отдел технических средств защиты.
5. Отдел защиты технологий платежных карточек.
6. Отдел охраны.
7. Режимно-секретный отдел.

Рассмотрим условия и состав работ каждого из отмеченных подразделений.

Отдел экономической безопасности банка (ОЭББ). Термин “экономическая безопасность” имеет много значений, часть из которых не входит в компетенцию данного отдела. Главной задачей отде-

ла является защита экономических интересов банка от противоправных посягательств и недобросовестной конкуренции путем сбора, обобщения и предоставления информации руководству банка для принятия решений по минимизации банковских рисков.

Работниками отдела при проведении кредитных операций проводятся мероприятия по предотвращению убытков банка и обеспечению доходности путем проведения проверок документов, кредитных и инвестиционных проектов, предоставленных заемщиками банка, мероприятий по осуществлению контроля над обоснованностью выдачи, использования, а также своевременности возвращения средств, выданных для реализации этих проектов.

Риск понести убытки от мошенничества в сфере кредитования может быть значительно снижен путем осуществления совокупности мер предосторожности, которые осуществляют работники отдела экономической безопасности.

Для реализации мер предосторожности работники банка выполняют следующие действия: проверяют подлинность сведений и документов, удостоверяющих право организации заключить договор займа в объеме и на условиях, предусмотренных проектом договора, а также подлинность документов, удостоверяющих личность руководителя или представителя организации, наличие у них соответствующих полномочий на получение кредита, правильность оформления доверенности и т.п. В особо важных случаях работники банковской безопасности снимают ксерокопии с предъявленного паспорта и доверенности с целью независимой проверки их подлинности, а также предлагают снабдить доверенность заверенной фотографией уполномоченного лица.

Работники банка получают сведения, подтверждающие реальное существование организации-заемщика путем изучения уставных документов, сведений из налоговых органов и других источников, устанавливают соответствие кредитуемой сделки законодательству и уставным документам заемщика. При выполнении указанных проверочных действий работники службы банковской безопасности не ограничиваются только изучением документов, а выполняют дополнительные мероприятия по сбору и анализу данных относительно заемщика. Напри-

мер, дополнительные сведения о реальном существовании организации-заемщика может дать информация о наличии у фирмы постоянных производственных и складских помещений, а также об объемах товаров или продукции, которыми располагает фирма.

Кроме того, работники службы банковской безопасности устанавливают наличие у заемщика способности заработать средства для погашения долга и возвратить кредит. С этой целью анализируются сведения о продолжительности присутствия фирмы на рынке товаров и услуг, о наличии положительных значений экономических показателей ее работы. Изучается кредитная история фирмы-заемщика: получал ли заемщик кредиты в других кредитных организациях, не допускал ли нарушений при их получении; как использовались деньги, полученные в качестве кредита; не было ли проблем с возвратом денег банку. Оценивается репутация фирмы-заемщика в деловом мире партнеров - контрагентов, кредиторов, банков.

Работники службы банковской безопасности проверяют достаточность вложения собственного капитала заемщика в кредитуемое дело (проект). О значении этих показателей можно судить по данным балансовых ведомостей, расчетно-кассовых документов и другой документации первичного учета. Соответствующим подтверждением добросовестности намерений заемщика может служить наличие у него достаточных объемов реального товара или продукции.

Работники службы банковской безопасности проводят тщательную юридическую и фактическую оценку подлинности документов во вторичных источниках погашения долга - договорах о залоге, гарантиях, поручительствах, страховых свидетельствах. В частности, проверяют их точное соответствие нормам гражданского законодательства, наличие возможных признаков материального и интеллектуального подлога.

После заключения кредитного договора работники банковской безопасности контролируют ход его выполнения с целью своевременного выявления обстоятельств, которые могут препятствовать возврату кредита. При возникновении таких обстоятельств работники службы банковской безопасности принимают меры к минимизации ущерба банка.

Предупреждение попыток проникновения в коллектив банка нежелательных лиц, а также возникновения неправомерных посягательств на персонал банка является частным направлением деятельности отдела экономической безопасности, который связан с выявлением и устранением угроз безопасности банка. Это объясняется тем, что такие попытки, как правило, представляют собой подготовительный этап к совершению преступных посягательств на имущество банка, на информацию и другие охраняемые объекты права собственности банка.

Для укомплектования банка персоналом кадровые подразделения банков используют специально разработанные методики. Такие методики включают:

- набор требований к деловым и личным характеристикам работников;
- описание процедур отбора и приема кандидатов на работу;
- рекомендации по планированию мероприятий по обучению, расстановке и воспитанию сотрудников;
- рекомендации и методику оценки профессиональных и личных качеств сотрудников;
- рекомендации по другим кадровым действиям.

Отдел работы с проблемной задолженностью банка (ОРПЗБ) занимается вопросами, связанными с так называемыми проблемными кредитами. Главной задачей отдела является решение вопроса возвращения проблемной задолженности в рамках действующего законодательства. Совместно с управлением кредитования кредитно-инвестиционного центра банка работники отдела определяет пути и формы погашения проблемной задолженности во всех филиалах системы банка. Для решения задач возвращения проблемной задолженности в рамках действующего законодательства организуется взаимодействие работников отдела, в первую очередь, с правоохранительными органами с целью их привлечения к работе по воздействию на должников и по возвращению в банк имеющейся проблемной задолженности. Для этого в рамках действующего законодательства проводится работа по поиску и идентификации должников и имущества, которое принадлежит каждому должнику.

Одним из вариантов возможного влияния на должников являются мероприятия по принудительному взысканию проблемной задолженности. Для этого проводятся действия по возмещению убытков от проведенных кредитных операций путем организации, координации и непосредственного оперативного осуществления мероприятий по возвращению кредитных средств. К таким мероприятиям относятся поиск руководителей юридических лиц - должников, установление местонахождения скрытых денежных средств и имущества должников, содействие государственным исполнителям в выполнении судебных решений.

Работники отдела также принимают участие в проведении периодических проверок документов по залогу и самого предмета залога с целью устранения возможных незаконных действий залогодателя относительно его реализации или повреждения в период действия кредитного договора и организации такой работы в региональных филиалах.

Отдел финансового мониторинга банка (ОФМБ). Основная задача отдела состоит в проведении внутреннего финансового мониторинга в банке.

Сотрудники отдела выполняют методические, контрольные и практические функции по выполнению мер по противодействию легализации (отмыванию) доходов, полученных преступным путем. Методические функции включают:

1. Разработку методических документов.
2. Обучение работников банка вопросам финансового мониторинга в рамках их служебных обязанностей.
3. Обобщение и распространение практического опыта проведения работы по противодействию легализации (отмыванию) доходов, полученных преступным путем.
4. Организацию делового взаимодействия с другими банками и структурами по вопросам финансового мониторинга.

Контрольные функции включают проведение проверок подразделений банка и его филиалов по вопросам соблюдения правил проведения внутреннего финансового мониторинга в банке. Практические функции предусматривают реализацию программ внутреннего

контроля в главном офисе и филиалах банка и оказание помощи в решении проблемных вопросов в случае их возникновения.

Работники отдела анализируют и обобщают информацию, которая поступает из информационных подсистем, применяемых в главном офисе.

Известные признаки, вызывающие подозрение о сомнительном характере финансовых операций, условно делятся на две группы:

1. Признаки, не свойственные имущественно-денежным операциям.
2. Признаки наличия схемы легализации.

Как правило, выявление признаков первой группы, не свойственных имущественно-денежным операциям, возможно еще на этапе имущественно-денежной операции и может осуществляться на уровне организаций первого уровня, реализующих эти операции.

Обнаружение признаков наличия схемы легализации возможно, как правило, только после осуществления цепочки связанных операций, реализующих эту схему, и в основном по информации, доступной уполномоченному органу финансовой разведки.

Признаки нетипичности операций указывают на потенциальную возможность применения имущественно-денежной операции в схемах по легализации незаконных доходов, но не указывают наличия самой схемы. Нетипичность операции устанавливают исходя из комбинации параметров ее признакового пространства, к которым могут относиться:

1. Вид основной деятельности компании, участвующей в операции; характер самой операции.
2. Географический фактор операции.
3. Особенности организационно-правовой формы участников (частная компания с учредителем престарелого или слишком молодого возраста).
4. События, непосредственно предшествующие операции (изменение состава собственников компании, получение компанией крупного кредита).
5. История движения денежных средств (от участника или к участнику операции).

Приведенный состав измерений признакового пространства не является раз и навсегда заданным. Он зависит от специфики условий

и может изменяться в зависимости от наличия источников информации об операции и от применяемой методики финансового мониторинга операций.

Примерами нетипичных финансовых операций могут быть:

1. Экономически необоснованные операции (технологически или экономически неоправданные покупки, продажи по заниженным ценам и др.).

2. Операции с участием слишком больших сумм или с нарушением привычного для деятельности организации ритма инкассации денежных средств.

Отнесение операции к типичным или нетипичным может основываться на историческом анализе для контрагентов операции и (или) сопоставительном - по виду деятельности, типу операции.

Информационными технологиями, которые позволяют реализовать поиск нетипичных операций, являются:

- *кластерный анализ.* Кластеры с незначительным числом объектов, а также граничные точки кластеров интерпретируются как “нетипичности” для рассматриваемого множества операций;
- *анализ временных рядов, регрессионное моделирование.* Роль нетипичностей в этом случае выполняют выбросы значений моделируемой переменной, например, сумма операций или частотные характеристики операций за определенный период.

Для больших объемов данных используются современные аналитические методы, такие как:

- деревья решений;
- нейронные сети.

Эти методы заключаются в построении оценочных алгоритмов, обучающихся на исторической информации. Настроенные алгоритмы оценки используются как фильтры для поиска нетипичностей в потоке новой информации из оперативных систем.

Характерной особенностью данных алгоритмов является необходимость их регулярной доработки на новых данных, что делает их максимально соответствующими текущей ситуации.

Эффективным направлением поиска и выявления нетипичностей схем операций является также комбинированное использование

отмеченных методов, при котором специалист-аналитик в процессе исследования сегментирует исходные данные на основе некоторого критерия, ищет функциональные зависимости в анализируемых данных в пределах выбранных сегментов, интерпретирует результаты и при необходимости повторяет анализ, изменив критерий сегментации.

Отдельная операция цепочки, рассматриваемая в отрыве от других операций, может не давать никаких оснований для возникновения подозрения, но все звенья цепочки в совокупности приобретают смысл функционального элемента схемы легализации.

Для цепочек операций, реализующих схему легализации, характерно наличие следующих признаков:

1. Закрепление за участниками схемы легализации ролей “стирщиков”, “отжимщиков”, “сушильщиков”.

2. Наличие определенной последовательности исполнения операций (сценарий осуществления схемы).

3. Синхронизация операций по времени (логистика исполнения сценария).

4. Согласованность суммы операции.

Основная цепочка операций может включать подчиненные цепочки операций, выполняющие отведенные им роли в общей схеме легализации, например, роль маскирования основной цепочки. Обнаружение признаков наличия схемы легализации является трудоемким процессом по ряду причин.

Во-первых, как правило, никогда заранее не ясно, по какой именно схеме может осуществляться легализация.

Во-вторых, на практике в реализации каждой схемы легализации возможны варианты: разрывы или опережения по времени между отдельными звеньями цепочки операций, нарушение порядка следования операций и т.д.

Ввиду указанных обстоятельств решение задачи обнаружения возможных схем легализации может выполняться методом прямого перебора с существенно большим количеством возможных вариантов схем легализации. Решение таких задач, даже с применением вычислительной техники, требует значительного времени и без активного

участия предметного специалиста, управляющего процедурой поиска, практически нереализуемо.

Информационные технологии, используемые при таком управляемом вычислительно-поисковом запросе, относятся к методам добывания данных, из которых преимущественное значение отводится методам анализа ассоциаций, выявления последовательности событий, анализа связей, поиска аналогий с использованием метода правдоподобных рассуждений.

При выявлении финансовых операций, которые имеют признаки обязательного финансового мониторинга, работники отдела регистрируют их и готовят сообщения в государственные органы финансового мониторинга об источниках и сути этих операций, а также о лицах, которые их осуществляют.

При выявлении финансовых операций, которые имеют признаки необходимости внутреннего финансового мониторинга, изучается тип, суть и цель этих финансовых операций, готовятся материалы по этим операциям для принятия решения ответственным работником.

В случае, если принимается решение о неподаче сообщения по этой операции в государственные органы финансового мониторинга, готовится справка, обосновывающая данное решение.

Если по поданным сообщения о выявленных финансовых операциях с признаками сомнительности поступают дополнительные запросы от государственных органов финансового мониторинга, работники отдела готовят материалы по этим запросам.

Кроме этого, работники отдела по полученным отчетам о проведенных финансовых операциях в филиалах банка осуществляют контроль над проведением в них финансового мониторинга.

Отдел технических средств защиты банка (ОТСЗБ). Центральной задачей отдела является:

1. Разработка основных направлений использования в банке технических и программных средств и способов защиты электронной банковской информации.

2. Генерация, учет и сохранение ключей и документов в подразделениях и филиалах банка.

3. Проведение анализа и организация работы по выявлению

возможных каналов утечки банковской информации с помощью технических средств защиты.

Работы по обеспечению информационной безопасности проводятся систематически и комплексно. Для этого используются защитные меры на законодательном, административном и программно-техническом уровнях.

Законодательный уровень является важнейшим для обеспечения информационной безопасности. При разработке системы обеспечения информационной безопасности банка особое внимание уделяется соответствию используемых управленческих решений, технологий, подходов и конкретных программно-аппаратных средств действующему законодательству. Для этого работниками отдела технических средств защиты выполняются мероприятия по тестированию программно-технических продуктов и проведению экспертиз на предмет их защиты от несанкционированного доступа, модификации и фальсификации информации.

Административный уровень реализуется в форме принятой политики безопасности. Политика безопасности представляет собой основные принципы и правила, соблюдение которых обеспечивает целостность и конфиденциальность информации. Принципы и правила политики безопасности излагаются в специальном документе, а также в пакете сопутствующих организационно-распорядительных документов. Эти документы охватывают все сферы деятельности банка и включают набор управленческих решений и инструкций, которые помогают банку совершать правильные действия, как в штатном режиме работы, так и в экстренных ситуациях.

Для соблюдения требований политики безопасности работники отдела предоставляют практическую и методическую помощь структурным подразделениям банка по вопросам защиты банковской информации в системе электронных платежей, электронного документооборота, технологий работы с банковскими платежными карточками, в программных и программно-технических комплексах, в телекоммуникационных системах. Работники отдела осуществляют контроль порядка использования, учета и хранения средств защиты электронной банковской информации в структурных подразделениях

главного офиса и филиалах банка, а также за выполнением персоналом требований информационной безопасности в корпоративных сетях банка, Интернете и в других системах.

Программно-технические меры образуют последний рубеж информационной защиты, который используют работники отдела. Средства безопасности, какими бы мощными и стойкими они ни были, сами по себе не могут гарантировать надежность программно-технического уровня защиты. Наиболее полную защиту обеспечивает корректно выполненная, проверенная на практике система взаимосвязанных мер. Такая система позволяет обеспечить эффективную и безопасную работу объединенных серверов безопасности, а также устойчивую управляемость информационной системы, возможность ее развития с одновременным противодействием новым угрозам при сохранении таких свойств, как высокая производительность, простота и удобство использования.

Для выполнения указанных требований работники отдела технических средств защиты собирают, обобщают и анализируют информацию по вопросам перспективного программно-технического обеспечения (криптографическое, аппаратное и программное обеспечение), информационной безопасности. По результатам такого анализа работники отдела технических средств защиты вносят предложения по внедрению перспективных программных и технических средств защиты в информационные системы региональных и подчиненных им филиалов банка.

Технология и результаты защиты информации в банковской автоматизированной системе имеют свои особенности, которые во многом определяют технологию информационной безопасности.

Отдел защиты технологий платежных карточек банка (ОЗТПКБ). Главной задачей отдела является осуществление контроля выполнения требований международных платежных систем по вопросам безопасности выпуска и обслуживания платежных карточек работниками банка. Кроме того, отдел принимает участие в планировании и реализации программ обеспечения безопасности при производстве, транспортировании, хранении, персонализации и обслуживании платежных карточек.

Программы предупреждения хищений средств банка с использованием пластиковых карточек, как правило, содержат комплекс мер организационного и технологического характера.

Организация выпуска карточек начинается с письменного согласования определенных мер между подразделениями, которые принимают участие в указанной процедуре. В процессе согласования инициатор выпуска готовит мотивированное предложение относительно изготовления карт.

Бухгалтерия подтверждает наличие средств на выпуск карты, отдел зашиты технологии платежных карт обеспечивает выполнение мероприятий по необходимым мерам защиты процесса изготовления и использования карточек, группа изготовления карточек готовит предложения производственно-технологического характера. Эти меры направлены на предотвращение возможного несанкционированного выпуска карточек.

В число организационных мер входит проведение предварительной проверки персональных данных будущих собственников пластиковых карточек и разработка рекомендаций для повышения надежности сохранения карточек. Соответствующие подразделения банка внимательно изучают и проверяют все организации-партнеры, которые предлагают выполнять обслуживание клиентов банка по пластиковым карточкам.

Меры технологического характера имеют своей целью повышение надежности процедуры передачи информации платежной системы и идентификации собственника карточки. Зарубежные банки для идентификации владельцев карт внедряют идентификационные системы с использованием биометрических параметров владельцев карт (голос, отражения пальцев рук и др.) и экономических параметров (число покупок, израсходованные суммы и др.).

Отдельным направлением деятельности работников отдела является обеспечение мер безопасности в процессе изготовления карточек и рассылки, обеспечение целости заготовок, расходных материалов, а также уже изготовленных карточек, соблюдение требований при делении уровней доступа к разным этапам изготовления карточек

с целью предельного ограничения числа лиц, осведомленных о внесенной в каждую карточку ключевой информации.

Еще одной функцией работников отдела является выявление противоправных действий сотрудников банка с использованием пластиковых карточек. Противоправные действия сотрудников банка с использованием пластиковых карточек могут быть следующими:

1. Неправомерное увеличение кредитного лимита на конкретную карточку и последующее хищение средств.

2. Несанкционированное установление в авторизационной системе специального статуса счета, который разрешает в определенных границах использовать деньги с карточки (разновидность кредитного лимита).

3. Несанкционированное пополнение счета карточки.

4. Выпуск равноценной карточки-двойника.

5. Несанкционированный выпуск новых пластиковых карт. Названные действия могут быть следствием не только злонамеренного умысла, но и результатом ошибки.

С целью реализации системы контроля работники отдела по указаниям руководства банка проводят служебные расследования в случаях мошенничества и злоупотреблений клиентов банка с использованием платежных карточек, в том числе и по просьбе других членов международных платежных систем. Кроме того, работники отдела пополняют уже существующий банк данных сведениями относительно лиц, которые неправомерно использовали платежные карточки, как на территории Российской Федерации, так и за ее пределами.

При этом проводятся мероприятия по установлению местонахождения лиц, которые имеют овердрафтные задолженности при использовании платежных карточек и оказывается содействие в возвращении денежных средств банка.

Отдел охраны банка (ООБ). Основной задачей отдела является организация и осуществление физической и технической охраны территории и помещений, денежных средств и материальных ценностей, обеспечение пропускного режима, контроль выполнения режима доступа работников банка к режимным помещениям, обслуживание охранно-пожарной сигнализации банка. В повседневной деятельности

работники отдела охраны проводят мероприятия по осуществлению пропускного режима, по контролю над доступом в хранилище банка, а также в помещения с ограниченным доступом.

Режимно-секретный отдел банка (РСОБ). Основной задачей отдела является недопущение необоснованного допуска и доступа лиц к сведениям, которые составляют государственную тайну. Такая задача возникает в случае, когда банк осуществляет финансовые операции, связанные с государственной тайной, или имеет в составе своих клиентов государственные структуры, во время работы с которыми используются документы, которые содержат государственную тайну. В соответствии с этой задачей работники отдела разрабатывают и реализуют вместе с другими структурными подразделениями банка мероприятия по обеспечению охраны государственной тайны, а также принимают меры по выявлению и закрытию каналов утечки государственных секретов в процессе деятельности банка.

Наибольшее количество нарушений, приводящих к утечке информации, содержащей государственную тайну, возможно в сфере традиционного документооборота. Поэтому работники отдела непрерывно контролируют соблюдение правил работы с грифованными документами. Кроме отмеченных задач, работники отдела выполняют задачи по охране коммерческой тайны.

Современный рынок банковских услуг характеризуется наличием многих его участников, интересы которых могут не совпадать и приводить к возможности противодействия, что порождает риск возникновения убытков. Кроме того, непредсказуемость развития рыночной ситуации является дополнительным источником риска. Поэтому рискованными оказывается большинство операций банка. Так как все управленческие решения банка и его конкурентов принимаются на основе конкретной информации, именно информационные риски являются одним из возможных источников возникновения убытков в деятельности банка.

Из опыта работы российских банков по обеспечению их информационной безопасности установлено наличие четырех основных видов информационных рисков банка:

1. Риск утечки и (или) разрушения необходимой для функцио-

нирования банка информации, в том числе такой информации, которая содержит государственную тайну или сведения конфиденциального характера.

2. Риск использования в деятельности банка информации, явно не соответствующей действительности.

3. Риск отсутствия у руководства банка объективной информации.

4. Риск распространения кем-либо во внешней среде информации, порочащей деловую репутацию банка или опасной для банка.

Количественная оценка типового соотношения информационных рисков позволяет утверждать, что риск утечки информации и риск распространения информации, невыгодной для банка, в сумме составляют более 50%. Следовательно, основные мероприятия защиты информации должны быть направлены на снижение именно этих видов информационных рисков банка.

Опыт показывает, что существенные потери в деятельности банка возникают при реализации угрозы утечки информации, составляющей банковскую или коммерческую тайну.

Особенностью банковской тайны является то, что в соответствии с законодательством обязанность охраны конфиденциальных сведений клиентов банка возложена на сам банк в связи со спецификой его деятельности. Поэтому деятельность банка по защите банковской тайны является его внутренней обязанностью, а по защите коммерческой тайны (сведений о деятельности самого банка) - законным правом банка.

Из опыта работы банка по защите банковской тайны от противоправных посягательств следует, что в зависимости от субъекта посягательства могут быть внешними и внутренними. Внешние посягательства осуществляются конкурирующими банками, криминальными элементами и другими заинтересованными в этом лицами, внутренние посягательства реализуются работниками банка, его акционерами и клиентами.

Таким образом, банковская безопасность действует по самым разнообразным направлениям, начиная от экономической безопасности, заканчивая организацией защиты и предупреждения физических угроз и угроз в сфере информационных технологий.

Глава 2.
МЕТОДЫ ОБЕСПЕЧЕНИЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ФИНАНСОВЫХ ОПЕРАЦИЙ ПРИ ИСПОЛЬЗОВАНИИ СРЕДСТВ ЭЛЕКТРОННОГО БАНКИНГА

2.1. Правовое обеспечение безопасности банковской деятельности

Правовые основы безопасности деятельности банка определяют соответствующие положения Конституции Российской Федерации, законы РФ от 5 марта 1992 г. № 2446-I в ред. от 26 июня 2008 г. «О безопасности», от 2 декабря 1990 г. № 395-1 в ред. Федерального закона от 13.07.2015 «О банках и банковской деятельности», Указ Президента Российской Федерации от 31 декабря 2015 года № 683 «О Стратегии национальной безопасности Российской Федерации» и другие нормативные акты. Правовая защита персонала, материальных и экономических интересов от преступных посягательств обеспечивается на основе норм Уголовного кодекса Российской Федерации (УК РФ) и Уголовно-процессуального кодекса Российской Федерации (УПК РФ), закона РФ от 17 января 1992 г. 2202-I в ред. Федерального закона от 28 ноября 2015 г. «О прокуратуре», Федерального закона от 3 апреля 1995 г. 40-ФЗ в ред. от 22 декабря 2014 г. «О федеральной службе безопасности», Федеральный закон от 07.02.2011 № 3-ФЗ (ред. от 13.07.2015) «О полиции», Федерального закона от 12 августа 1995 г., 144-ФЗ в ред. от 29.06.2015 г. «Об оперативно-розыскной деятельности», закона РФ от 11 марта 1992 г. 2487-I в ред. от 13.07.2015

«О частной детективной и охранной деятельности», Федерального закона от 13 декабря 1996 г. № 150-ФЗ «Об оружии» и др.

Защиту имущественных и иных материальных интересов и деловой репутации призваны обеспечивать также гражданское, гражданско-процессуальное, арбитражное, арбитражно-процессуальное и трудовое законодательство. Так, в соответствии с нормами гл. 39 Трудового кодекса Российской Федерации (ТК РФ) работники инкассации несут материальную ответственность за сохранность денег и других ценностей, принятых ими для доставки по назначению. В случае утери или хищения ценностей материальная ответственность по возмещению причиненного вреда возлагается солидарно на всех членов бригады, ответственных за доставку ценностей. С членами бригады заключается договор о коллективной (бригадной) материальной ответственности.

Статья 139 Гражданского кодекса Российской Федерации (ГК РФ) предусматривает условия защиты информации, составляющей служебную, банковскую и коммерческую тайны. Гражданский кодекс Российской Федерации рассматривает конфиденциальную информацию как самостоятельный объект правоотношений. Право на конфиденциальную информацию включает в себя: право на обладание и пользование информацией; право на воспроизведение и распространение информации; право на уничтожение и защиту информации.

Статья 26 Федерального закона «О банках и банковской деятельности» предусматривает режим получения различными органами, юридическими и физическими лицами информации, содержащей банковскую тайну. В соответствии с указанной статьей режим банковской тайны устанавливает строго ограниченный и исчерпывающий перечень лиц и оснований, имеющих право на получение информации, относящейся к банковской тайне.

Обеспечение информационной безопасности регулируется Законом РФ от 12 июля 1993 г. 5485-I в ред. от 08.03.2015 «О государственной тайне», Федеральным законом от 20 февраля 1995 г. № 24-ФЗ в ред. от 31.12.2014 «Об информации, информатизации и защите информации».

Важное значение имеют указы Президента Российской Федерации от 8 мая 1993 г. № 644 «О защите информационно-телекоммуникационных систем и баз данных от утечки конфиденциальной информации по техническим каналам», от 3 апреля 1995 г. № 334 «О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации», от 5 января 1992 г. № 9 «О создании Государственной технической комиссии при Президенте Российской Федерации». При практическом решении задач обеспечения безопасности банка необходимо опираться также на следующие правовые нормативные акты:

- постановление Правительства РСФСР от 5 декабря 1991 г. № 35 «О перечне сведений, которые не могут составлять коммерческую тайну»;
- положение о сертификации средств защиты информации, утвержденное постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608;
- указ Президента Российской Федерации от 3 июня 1997 г. № 188 «О конфиденциальной информации»;
- положение о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам, утвержденное постановлением Правительства РФ от 15 сентября 1993 г. № 912-51;
- положение о государственном лицензировании деятельности в области защиты информации, утвержденное совместным решением Гостехкомиссии и ФАПСИ при Президенте Российской Федерации от 27 апреля 1994 г. № 10.

Существующие правовые условия обеспечения безопасности, в основном, позволяют государственным и иным правоохранительным и охранным структурам организовывать противодействие противоправным посягательствам на предпринимательскую деятельность в различных ее сферах.

В соответствии с законодательством Российской Федерации и нормами права в части обеспечения информационной безопасности, требованиями нормативных актов Центрального банка Российской

Федерации, федерального органа исполнительной власти, уполномоченного в области безопасности, федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации, разрабатывается Политика коммерческого банка в сфере информационной безопасности (далее – Политика). При ее разработке необходимо учитывать Доктрину информационной безопасности Российской Федерации (от 09.09.2000 Пр-1895); Стандарт Банка России СТО БР ИББС -1.0 – 2010 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации.

Политика является документом, доступным любому сотруднику Банка и пользователю его ресурсов, представляет собой официально принятую руководством Банка систему взглядов на проблему обеспечения информационной безопасности и устанавливает принципы построения системы управления информационной безопасностью на основе систематизированного изложения целей, процессов и процедур информационной безопасности Банка.

Руководство Банка осознает важность и необходимость развития и совершенствования мер и средств обеспечения информационной безопасности в контексте развития законодательства и норм регулирования банковской деятельности, а также развития реализуемых банковских технологий и ожиданий клиентов Банка и других заинтересованных сторон. Соблюдение требований информационной безопасности позволит создать конкурентные преимущества Банку, обеспечить его финансовую стабильность, рентабельность, соответствие правовым, регулятивным и договорным требованиям и повышение имиджа.

Требования информационной безопасности, которые предъявляются Банком, соответствуют интересам (целям) деятельности Банка и предназначены для снижения рисков, связанных с информационной безопасностью, до приемлемого уровня. Факторы рисков в информационной сфере Банка имеют отношение к его корпоративному управлению (менеджменту), организации и реализации бизнес-процессов, взаимоотношениям с контрагентами и клиентами, внутрихозяйственной деятельности.

Факторы рисков в информационной сфере Банка составляют значимую часть операционных рисков Банка, а также имеют отношение и к иным рискам основной и управленческой деятельности Банка.

Стратегия Банка в области обеспечения информационной безопасности и защиты информации наряду с прочим включает выполнение в практической деятельности требований:

1. Российского законодательства в области безопасности, безопасности информационных технологий и защиты информации, безопасности персональных данных, банковской тайны и других правовых актов.

2. Нормативных актов федеральных органов исполнительной власти, уполномоченных в области обеспечения физической безопасности и технической защиты информации, противодействия техническим разведкам и обеспечения информационной безопасности и приватности.

3. Нормативных актов Банка России и стандартов Банка России по обеспечению информационной безопасности из комплекса стандартов «СТО БР ИББС».

4. Нормативных актов Банка России и документов Банка России в области стандартизации «Обеспечение информационной безопасности организаций банковской системы Российской Федерации», утвержденных распоряжением Банка России от 21 июня 2010 г.

Необходимые требования обеспечения информационной безопасности Банка должны неукоснительно соблюдаться персоналом Банка и другими сторонами, как это определяется положениями внутренних нормативных документов Банка, а также требованиями договоров и соглашений, стороной которых является Банк.

Положения данного документа распространяются на бизнес - процессы Банка и обязательны для применения всеми сотрудниками и руководством Банка, а также пользователями его информационных ресурсов. Эти положения должны быть учтены при разработке политик информационной безопасности в дочерних и аффилированных организациях.

Политика коммерческого банка в сфере информационной

безопасности в соответствии с рекомендациями в области стандартизации Банка России РС БР ИББС 2.0 2007 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методические рекомендации по документации в области обеспечения информационной безопасности в соответствии с требованиями СТО БР ИББС 1.0», принятыми и введенными в действие распоряжением Банка России от 28 апреля 2007г. № Р-348, является корпоративным документом по ИБ первого уровня. Документами, детализирующими положения корпоративной Политики применительно к одной или нескольким областям ИБ, видам и технологиям деятельности Банка, являются частные политики по обеспечению ИБ (далее – Частные политики), которые являются документами по ИБ второго уровня, оформляются как отдельные внутренние нормативные документы банка, разрабатываются и согласовываются в соответствии с установленным в банке порядком, утверждаются куратором.

В соответствии с Политикой основными объектами защиты системы информационной безопасности в банке являются:

• информационные ресурсы, содержащие коммерческую тайну, банковскую тайну, персональные данные физических лиц, сведения ограниченного распространения, а также открыто распространяемая информация, необходимая для работы банка, независимо от формы и вида ее представления;

• информационные ресурсы, содержащие конфиденциальную информацию, включая персональные данные физических лиц, а также открыто распространяемая информация, необходимая для работы банка, независимо от формы и вида ее представления;

• сотрудники банка, являющиеся разработчиками и пользователями информационных систем банка;

• информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены такие системы.

Целью деятельности по обеспечению информационной безопасности банка является снижение угроз информационной безопасности до приемлемого для банка уровня. Основные задачи деятельности по обеспечению информационной безопасности банка:

• выявление потенциальных угроз информационной безопасности и уязвимостей объектов защиты;

• предотвращение инцидентов информационной безопасности;

• исключение либо минимизация выявленных угроз.

Составной частью Политики выступает модель нарушителя информационной безопасности. По отношению к банку нарушители могут быть разделены на внешних и внутренних нарушителей. В качестве потенциальных внутренних нарушителей банком рассматриваются:

• зарегистрированные пользователи информационных систем банка;

• сотрудники банка, не являющиеся зарегистрированными пользователями и не допущенные к ресурсам информационных систем банка, но имеющие доступ в здания и помещения;

• персонал, обслуживающий технические средства корпоративной информационной системы банка;

• сотрудники самостоятельных структурных подразделений банка, задействованные в разработке и сопровождении программного обеспечения;

• сотрудники самостоятельных структурных подразделений, обеспечивающие безопасность банка;

• руководители различных уровней.

В качестве потенциальных внешних нарушителей Банком рассматриваются:

• бывшие сотрудники банка;

• представители организаций, взаимодействующих по вопросам технического обеспечения банка;

• клиенты банка;

• посетители зданий и помещений банка;

• конкурирующие с банком кредитные организации;

• члены преступных организаций, сотрудники спецслужб или лица, действующие по их заданию;

• лица, случайно или умышленно проникшие в корпоративную информационную систему банка из внешних телекоммуникационных сетей (хакеры).

В отношении внутренних и внешних нарушителей принимаются следующие ограничения и предположения о характере их возможных действий:

• нарушитель скрывает свои несанкционированные действия от других сотрудников банка;

• несанкционированные действия нарушителя могут быть следствием ошибок пользователей, эксплуатирующего и обслуживающего персонала, а также недостатков принятой технологии обработки, хранения и передачи информации;

• в своей деятельности вероятный нарушитель может использовать любое имеющееся средство перехвата информации, воздействия на информацию и информационные системы, адекватные финансовые средства для подкупа персонала, шантаж, методы социальной инженерии и другие средства и методы для достижения стоящих перед ним целей;

• внешний нарушитель может действовать в сговоре с внутренним нарушителем.

Неисполнение или некачественное исполнение сотрудниками Банка и пользователей информационных систем обязанностей по обеспечению информационной безопасности может повлечь лишение доступа к информационным системам, а также применение к виновным административных мер воздействия, степень которых определяется установленным в банке порядком либо требованиями действующего законодательства.

Стратегия банка в части противодействия угрозам информационной безопасности заключается в сбалансированной реализации взаимодополняющих мер по обеспечению безопасности: от организационных мер на уровне руководства банка, до специализированных мер информационной безопасности по каждому выявленному в банке риску, основанных на оценке рисков информационной безопасности. С целью поддержки заданного уровня защищенности банк придерживается процессного подхода в

построении системы менеджмента информационной безопасности. Система менеджмента информационной безопасности банка основывается на осуществлении следующих основных процессов (планирование, реализация и эксплуатация защитных мер, проверка (мониторинг и анализ), совершенствование) соответствующих требованиям стандарта Банка России СТО БР ИББС–1.0 и положениям международных стандартов по обеспечению информационной безопасности. Реализация этих процессов осуществляется в виде непрерывного цикла – «планирование – реализация – проверка – совершенствование – планирование – …», направленного на постоянное совершенствование деятельности по обеспечению информационной безопасности банка и повышение ее эффективности. На всех этапах жизненного цикла управление информационной безопасностью банка осуществляется с соблюдением нормативных документов, определяющих процессы управления операционными рисками банка.

При планировании мероприятий по обеспечению информационной безопасности в банке осуществляются:

1. Определение и распределение ролей персонала банка, связанного с обеспечением информационной безопасности (ролей информационной безопасности).

2. Оценка важности информационных активов с учетом потребности в обеспечении их свойств с точки зрения информационной безопасности.

3. Менеджмент рисков информационной безопасности, включающий:

• анализ влияния на информационную безопасность банка применяемых в деятельности Банка технологий, а также внешних по отношению к банку событий;

• выявление проблем обеспечения информационной безопасности, анализ причин их возникновения и прогнозирование их развития;

• определение моделей угроз информационной безопасности;

• выявление, анализ и оценка значимых для банка угроз информационной безопасности;

Таким образом, Политика информационной безопасности банка включает:

• выявление возможных негативных последствий для банка, наступающих в результате проявления факторов риска информационной безопасности, в том числе связанных с нарушением свойств безопасности информационных активов банка;

• идентификацию и анализ рисковых событий информационной безопасности;

• оценку величины рисков информационной безопасности и определение среди них рисков, неприемлемых для банка;

• обработку результатов оценки рисков информационной безопасности, базирующейся на методах управления операционными рисками, определенных в банке;

• оптимизацию рисков информационной безопасности за счет выбора и применения защитных мер, противодействующих проявлениям факторов риска и минимизирующих возможные негативные последствия для банка в случае наступления рисковых событий;

• оценку влияния защитных мер на цели основной деятельности банка;

• оценку затрат на реализацию защитных мер;

• рассмотрение и оценку различных вариантов решения задач по обеспечению информационной безопасности;

• разработку планов управления рисками, предусматривающих различные защитные меры и варианты их применения, и выбор из них такого, реализация которого максимально положительно скажется на целях основной деятельности банка и будет оптимальна с точки зрения произведенных затрат и ожидаемого эффекта;

• документальное оформление целей и задач обеспечения информационной безопасности банка, поддержка в актуальном состоянии нормативно – методического обеспечения деятельности в сфере информационной безопасности.

В рамках реализации деятельности по обеспечению информационной безопасности в банке осуществляются: менеджмент инцидентов информационной безопасности, включающий сбор

информации о событиях информационной безопасности, выявление и анализ инцидентов информационной безопасности, расследование инцидентов информационной безопасности; оперативное реагирование на инцидент информационной безопасности; минимизация негативных последствий инцидентов информационной безопасности; оперативное доведение до руководства банка информации по наиболее значимым инцидентам информационной безопасности и оперативное принятие решений по ним, включая регламентирование порядка реагирования на инциденты информационной безопасности; выполнение принятых решений по всем инцидентам информационной безопасности в установленные сроки; пересмотр применяемых требований, мер и механизмов по обеспечению информационной безопасности по результатам рассмотрения инцидентов информационной безопасности; повышение уровня знаний персонала банка в вопросах обеспечения информационной безопасности; обеспечение регламентации и управления доступом к программным и программно-техническим средствам и сервисам автоматизированных систем банка и информации, обрабатываемой в них; применение средств криптографической защиты информации; обеспечение бесперебойной работы автоматизированных систем и сетей связи; обеспечение возобновления работы автоматизированных систем и сетей связи после прерываний и нештатных ситуаций; применение средств защиты от вредоносных программ; обеспечение информационной безопасности на стадиях жизненного цикла автоматизированных систем банка, связанных с проектированием, разработкой, приобретением, поставкой, вводом в действие, сопровождением (сервисным обслуживанием); обеспечение информационной безопасности при использовании доступа в сеть Интернет и услуг электронной почты; контроль доступа в здания и помещения банка.

Обеспечение защиты информации от утечки по техническим каналам включает: применение мер и технических средств, снижающих вероятность несанкционированного получения информации в устной форме - пассивная защита; применение мер и технических средств, создающих помехи при несанкционированном

получении информации - активная защита; применение мер и технических средств, позволяющих выявлять каналы несанкционированного получения информации - поиск.

В целях проверки деятельности по обеспечению информационной безопасности в банке осуществляются: контроль правильности реализации и эксплуатации защитных мер; контроль изменений конфигурации систем и подсистем банка; мониторинг факторов рисков и соответствующий их пересмотр; контроль реализации и исполнения требований сотрудниками банка действующих внутренних нормативных документов по обеспечению информационной безопасности банка; контроль деятельности сотрудников и других пользователей информационных систем банка, направленный на выявление и предотвращение конфликтов интересов.

Предложенное содержание Политики коммерческого банка в сфере информационной безопасности должно быть адаптировано к особенностям функционирования данной кредитной организации. При этом в целях совершенствования деятельности по обеспечению информационной безопасности в банке должно осуществляться периодическое, а при необходимости оперативное, уточнение/пересмотр целей и задач обеспечения информационной безопасности (при изменениях целей и задач основной деятельности банка).

2.2. Применение современных информационных технологий в банковской сфере

Информационные технологии в банковской сфере имеют определенные цели, методы и средства реализации. Целью информационной технологии является создание из информационного ресурса качественного информационного продукта, удовлетворяющего требования пользователя. Методами информационных технологий являются методы и приемы моделирования, разработки и реализации процедур обработки данных. В качестве средств информационных технологий применяются математические методы и модели решения задач, алгоритмы обработки данных, инструментальные средства моделирования

бизнес- процессов, данных, проектирования информационных систем, разработки программ, собственно программные продукты, разнообразные информационные ресурсы, технические средства обработки данных. Главная отличительная особенность информационных технологий заключается в их целевой направленности на оптимизацию информационных процессов, выходным результатом которых является информация.

Информационная банковская технология – процесс преобразования банковской информации на основе методов сбора, регистрации, передачи, хранения и обработки данных в целях обеспечения подготовки, принятия и реализации решений. В финансово-кредитной системе информационная банковская технология способствует своевременному и качественному выполнению банковских функций, а также значительно повышают уровень управления как банковской системы в целом, так и каждым банком и практически реализуется в автоматизированных банковских системах.

Перспективное направление развития автоматизированных банковских технологий как у нас в стране, так и за рубежом – шестое поколение АБС. Шестое поколение: аппаратная платформа – гетерогенная сетевая среда; СУБД – профессиональные реляционные с открытым интерфейсом (возможно одновременно несколько разных СУБД); базовый элемент технологии – сделка или документ; структура АБС – логические АРМ, динамически формируемые по компонентной технологии, сильно связанные по данным и функциям в пределах всей сети Интернет.

Одним из ключевых направлений развития банковской системы Российской Федерации и мировой банковской системы выступает ее модернизация на основе внедрения достижений науки и техники. Это обусловлено превращением процессных и продуктовых инноваций в ключевой фактор повышения эффективности управления информационными ресурсами в банковском секторе. Развитие информационных технологий позволяет в значительной степени сократить дистанцию между производителем и потребителем банковских услуг, стимулирует межбанковскую конкуренцию, а следовательно, способствует развитию банковского обслуживания. Их внедрение в деятельность бан-

ковских организаций обеспечивает повышение уровня конкурентоспособности банков на национальном и мировом рынках и одновременно создает дополнительные источники угроз для их деятельности.

Современная система электронного банкинга включает два основных направления:

1. B2B (business-to-business), где банки работают в качестве основного исполнителя и продавца финансовых услуг.

2. B2C (business-to- customer) — продажа товаров и услуг частным лицам, где кредитные организации выступают в роли финансового посредника.

Важнейшей тенденцией, связанной с расширением оперативности и многофункциональности кредитных организаций, явилось создание систем бюджетирования и комплексный подход к финансовому менеджменту ресурсами банка[1]. Помимо собственно программного обеспечения, банковские информационные технологии решают еще целый комплекс задач, касающихся информационного и аппаратно-технического обеспечения банковских операций.

В качестве основных функциональных направлений банковских информационных технологий выступают:

• информационные технологии для ведения бухгалтерского учета, которые должны обеспечить обработку операций, проводимых банком, с приемлемой степенью скорости и надежности, осуществлять всю бухгалтерскую и финансовую отчетность, а также должны автоматизировать реальный банковский документооборот;

• информационные технологии для управленческого учета и стратегического планирования, которые обеспечивают эффективный контроль и анализ управленческой и учетной информации, а также обмен данными с программными продуктами и инструментальными средствами для финансового и статистического анализа;

• информационные технологии для передачи информации, которые включают: электронно-расчетные межбанковские системы, системы электронной связи отделений и филиалов банка с головным офисом.

---

[1] Черкасова Е.А. Информационные технологии в банковском деле: учеб. пособие. М.: Академия, 2011. 320 с.

Можно выделить следующие инновационные направления банковских информационных технологий:

• мобильные финансовые сервисы и оптимизация рынка микроплатежей;

• предиктивная аналитика и внедрение новых моделей управления рисками;

• кибернетика и информационная безопасность;

• оптимизация собственных бизнес-процессов и увеличение скорости внедрения инноваций (от аутсорсинга до построения инновационных консорциумов банков и ИТ-компаний);

• развитие форм дистанционного банковского обслуживания;

• повышение управляемости банком — системы ERP, CRM, BI, BP внедрение клиентоориентированной модели бизнеса[1].

В настоящее время в Российской Федерации представлены программные продукты как отечественных, так и зарубежных разработчиков, предлагаемые системы отличаются в несколько раз по своей стоимости и функциональности. Укрупнение банковского бизнеса в России способствовало приходу на этот рынок западных поставщиков с масштабными и дорогостоящими решениями (mySAP Ba№ki№g, T24от «Teme№os», OFSA от «Oracle» и др.). В то же время улучшается качество автоматизированных систем, предлагаемых на рынке отечественными разработчиками. Отечественные системы в настоящее время предоставляют достаточно полный набор функций, поддержку изменений требований Банка России к учету и отчетности. Системы последнего поколения могут конкурировать с зарубежными в части гибкости, настраиваемости и архитектурных решений.

К числу новых тенденций в сфере электронного банкинга относятся:

1. Слияние банковских и информационных технологий и рождение новой отрасли — финансово-технологической.

2. Персонификация продуктов и услуг.

3. Применение облачных решений как рабочего инструмента для оптимизации затрат и повышения эффективности.

---

[1] Цифровому банку будущего быть! URL: http://www.bps-sberbank.by/online/ru.about.news.201510290841-html (дата обращения: 20.07.2017).

4. Совершенствование методов и инструментария борьбы с техническим взломом, эксплойтами, DoS- и DDoS-атаками, разработка мер защиты отдельных приложений и информационных систем.

5. Рост востребованности удаленных сервисов и дистанционного банковского обслуживания.

6. Повышение роли call- и контакт-центров, их модернизация.

7. Приведение системы защиты платежной информации в соответствие с требованиями Федерального закона 161-ФЗ «О национальной платежной системе». Вхождение Банка России в состав ассоциации XBRL International вызвало увеличение спроса на доработку банковского софта.

8. Использование новых средств идентификации клиентов, использование датчиков сканирования отпечатка пальца для входа в мобильные приложения.

9. Интеграция собственных систем банков.

10. Разработка инструментов взаимодействия инфраструктуры отдельного банка с сетями провайдеров облачных сервисов и интернета.

11. Доработка интеграционных процессов в разных банках под единый бизнес-процесс.

12. Создание цифрового банка.

13. Эволюция мобильного и интернет-банкинга приведет к необходимости создания уникальной корпоративной социальной мультисреды, доступной и сотрудникам, и клиентам, или банковской экосистемы.

14. Наряду с использованием роботов-консультантов, владеющих с речевыми технологиями и простыми формами искусственного интеллекта для помощи в решении несложных вопросов, а также роботоэдвайзеров для автоматического управления инвестициями, предполагается внедрение систем искусственного интеллекта, способных самообучаться и помогать принимать сложные решения на основе обработки больших массивов данных.

15. Широкое внедрение риск-менеджмента и стандартов достаточности банковского капитала «Базель III» (переход на «Базель III» должен быть осуществлен в мировом масштабе к 2019 году). Эволюция методов и принципов функционирования банковских организа-

ций, которые были сформулированы Базельским комитетом по банковскому надзору, созданным ЦБ стран G10 в 1975 году после серии банкротств крупных финансовых институтов, представлена на рис. 1. Указанные принципы используются и в Российской Федерации.

Рис. 1. Принципы управления банковскими рисками в соответствии с решениями Базельского комитета по банковскому надзору

Направления изменения механизма управления банковскими рисками, разработанные Центральным банком Российской Федерации, представлены на рис. 2.

Рис. 2. Направления изменения механизма инструментов управления банковскими рисками, разработанные Центральным банком Российской Федерации

Методы управления банковскими рисками представлены на рис. 3.

Рис. 3. Методы управления банковскими рисками

Управленческие технологии, используемые в отношении отдельных видов риска, представлены на рис. 4.

Рис. 4. Методы управления фондовым, процентным и операционным рисками, рисками ликвидности

По данным компании IDC, расходы на ИТ в банковском секторе составили в 2016 году 480 млрд долл. США, что на 4,2 больше аналогичного показателя в 2015 г.[1] Рост расходов обусловлен ростом влияния третьей технологической платформы: облачных технологий, мобильных приложений и решений в области Big Data. В сфере управления финансовыми рисками объем расходов на ИТ составил порядка $85 млрд. ПАО «Сбербанк России» стал самым информатизованным банком в 2014 году, опередивший ВТБ, который занимал первую строчку годом ранее. Заметный рывок вперед сделал Юникредит Банк, переместившийся с 11 на 7 место. Новичок рейтинга – Россельхозбанк - оказался сразу на 6 месте[6].

В настоящее время на рынках используются три основных варианта интернет-банкинга: информационный, коммуникационный и операционный.

[1] Официальный сайт компании International Data Corporation (IDC). URL: http://idcrussia.com/ru/ (дата обращения: 20.07.2017).

Информационный интернет-банкинг – это базовый уровень интернет-банкинга. Как правило, банк при этом дает маркетинговую информацию относительно банковских услуг и обслуживания на обособленном сервере. Сопутствующие риски в данном случае относительно низки, поскольку родственной связи между таким сервером и внутренней вычислительной сетью банка нет.

Коммуникационный интернет-банкинг. Этот тип системы позволяет реализовать некоторые виды взаимодействия между системами конкретного банка и его клиентом. Такое взаимодействие может быть ограничено электронной почтой, запросами справок о счетах, заявками на ссуды или обновлением стандартных файлов (изменение имени и адреса). Например, некоторые банки предоставляют услуги по предварительному автоматическому рассмотрению заявок на выдачу кредита, консультированию по вопросам управления портфелем ценных бумаг на основе автоматизации решающих правил технического анализа.

Операционный интернет-банкинг. Данный уровень интернет-банкинга позволяет клиентам выполнять трансакции. Поскольку обычно существует непосредственная связь с сервером и внутренней вычислительной сетью банка или обслуживающей его организации, такой архитектуре сопутствует наивысший риск, и в ней должны присутствовать серьезные средства контроля. Трансакции клиента могут включать доступ к счетам, осуществление платежей, перевод средств и т.д.

В ряде случаев банки с помощью Интернета проводят операции по размещению привлеченных денежных средств. Принципиально возможны выдача банковских гарантий, а также привлечение во вклады и размещение драгоценных металлов при условии их физического депонирования в некоем хранилище. При осуществлении интернет-банкинга пока технологически и законодательно не решены вопросы проведения операций, непосредственно связанных с движением наличных денежных средств.

Наиболее популярная модель – это использование интернет-банкинга в качестве канала продаж. В этом случае электронный банкинг

является дополнительным каналом к основному бизнесу банка и действует под тем же брендом. Этой модели придерживаются Citiba№k и Deutsche Ba№k.

Вторая модель предполагает выделение электронного банкинга в отдельный бизнес, работающий под собственным брендом (в Германии такие финансовые учреждения называют директ-банками). По такому пути пошли First Direct (отдельный бренд HSBC), Comdirect (бренд, принадлежащий Commerzbank), MBank (соответствует Bre Bank SA).

Третья модель подразумевает создание нового электронного бизнеса, у таких компаний конкуренция с основным бизнесом отсутствует. Примером реализации этой стратегии служат DiBa и Egg.

Существует также и четвертая модель интернет-банкинга – агрегатор электронного финансового супермаркета (банк, осуществляющий web-продажи как своих, так и предлагаемых другими финансовыми институтами услуг).

Наиболее распространенными являются первые две модели, причем интернет-подразделение обычно используется для операций на внутреннем финансовом рынке, а интернет-банк – для выхода за границу (в первую очередь на рынки развивающихся стран), поскольку именно он обеспечивает необходимую для зарубежной деятельности гибкость в использовании инструментов, установлении тарифов и отборе клиентов.

Специфика технологии интернет-банкинга приводит к существенным изменениям в профилях риска использующих ее банков, к расширению состава и увеличению степени влияния факторов того или иного банковского риска. Интернет-банкинг не меняет природы финансовых рисков. При его проведении банкам приходится сталкиваться с теми же основными видами риска, что и при проведении классических банковских операций (кредитный, ликвидности, рыночный, операционный, правовой). При этом интернет-банкинг, как правило, на современном технологическом уровне увеличивает подверженность риску и вносит разнообразие в его структуру, что обусловлено:

– виртуальным характером дистанционных банковских операций;

– общедоступностью «открытых» телекоммуникационных систем;

– чрезвычайно высокой скоростью выполнения трансакций;

– глобальными масштабами межсетевого операционного взаимодействия;

– активным участием фирм – провайдеров услуг в проведении операций.

При идентификации и анализе рисков интернет-банкинга необходимо учитывать все компоненты среды, через которые проходят банковские данные кредитной организации и информация ее клиентов, поскольку каждый из этих компонентов в той или иной мере может оказаться источником риска. Классификация банковских рисков предсиавлена на рис. 5.

Классификационный признак	Тип риска	Вид банковского риска
По основному содержанию деятельности	Кредитный риск	
	Валютный риск	
	Процентный риск	
	Риск по формированию депозитов	
	Риск ликвидности	
	Репутационный риск	
	Риск неплатежеспособности (банкротства)	
	Операционные риски	Риск нарушения законодательства
		Риск противоправных действий или злоупотреблений сотрудников
		Риск противоправных действий контрагентов
		Риск нарушения администрацией банка или сотрудниками трудового законодательства
		Другие типовые операционные риски
По сфере возникновения	Внешние риски	Страновой риск
		Валютный риск
		Правовый (законодательный) риск
		Отраслевой риск
		Риск форс-мажорных обстоятельств
	Внутренние риски	Риски, связанные с видом банка
		Риски, связанные с характером банковских операций
		Риски, связанные со спецификой деятельности клиентов банка
По степени воздействия	Низкие	
	Умеренные	
	Полные	
По причине возникновения	Чистые	
	Спекулятивные	
По форме проявления	Системные	
	Несистемные	
По возможности управления	Открытые	
	Незакрытые	

Рис. 5. Классификация банковских рисков

К рискам, связанным с интернет-банкингом, с разной степенью воздействия относят: кредитный, процентный, фондовый, валютный, операционный, стратегический, репутационный, правовой, а также риск ликвидности. При этом указанный перечень рисков не является исчерпывающим.

Кредитный риск обнаруживается во всех видах деятельности, в которых успех зависит от действия партнера, эмитента или заемщика. Он возникает каждый раз, когда фонды банка распределяются, передаются или иным образом подвергаются опасности через явные или подразумеваемые контрактные соглашения, независимо от того, учитываются они на балансе или вне баланса. Кредитный риск имеет место в кредитных организациях, уровень использования интернет-банкинга в которых высок, в частности, в использовани электронного банкинга для выдачи кредитов.

Процентный риск возникает в процессе онлайн-трейдинга, поскольку в этом случае операции управляются трейдерами, не зависящими от банковской системы управления, а также при предоставлении депозитных и кредитных продуктов клиентам через Интернет.

Риск ликвидности. Увеличение риска ликвидности может быть связано с предоставлением клиентам возможности оперативно и круглосуточно выполнять перевод средств по счетам, открытым в различных банках. Увеличение мобильности капитала приводит к повышению волатильности депозитных счетов. При этом концентрация риска ликвидности зависит от объема и характера действий со счетами, контролируемыми клиентами через Интернет, что, соответственно, оказывает влияние на выстраиваемую банком систему мониторинга ликвидности и изменений в депозитах и ссудах.

Фондовый риск. Банки могут подвергаться фондовому риску, если они начинают или расширяют депозитный брокеринг, торговлю кредитами или программу страхования от риска в результате деятельности в рамках интернет-банкинга. Риск финансовых инструментов, с которыми банк проводит операции, может возрасти под влиянием развития еще одного направления деятельности на финансовом рынке – интернет-трейдинга. Соответственно, если осуществляется активный трейдинг, банку следует обеспечивать наличие необходимых систем управления для мониторинга, измерения фондового риска и управления им.

Валютный риск имеет место, когда некая ссуда или кредитный портфель номинируется в валюте или финансируется за счет займов в

другой валюте. Валютный риск может увеличиться за счет действия политических, социальных или экономических факторов.

Операционный риск. Наибольшую угрозу для банка при оказании им услуг через Интернет представляет операционный риск. Он проявляется в каждой интернет-услуге и распространяется на организацию услуг и их предоставление, обработку трансакций, разработку систем, на компьютерные системы, сложность услуг и обслуживания, а также на условия осуществления внутреннего контроля.

Банки, предоставляющие услуги и обслуживание через Интернет, должны гарантировать, что им удалось организовать оптимальное сочетание услуг при их высокой надежности и своевременности как факторов положительной деловой репутации.

Банкам, которые предлагают оплату счетов через Интернет, потребуется построение процесса для осуществления клиринга трансакций между самим банком, его клиентами и третьими сторонами. Следует понимать, что ошибки в клиринге могут усугубить репутационный риск, риск ликвидности и кредитный риск банка.

При рассмотрении операционного риска, как правило, наибольшее внимание уделяется вопросам безопасности. Использование банками современных криптографических систем, соответствующих компьютерных программ и других средств позволяет достигнуть надлежащего уровня безопасности. Для обеспечения эффективности системы информационной безопасности необходимо предусмотреть в соответствующих внутрибанковских регламентах и процедурах порядок их использования, а также порядок действий в непредвиденных ситуациях. При этом система регламентов деятельности входящих в ее состав подразделений должна постоянно изменяться с учетом факторов внешней и внутренней среды. Система внутреннего контроля обеспечивает выполнение указанных регламентов. Кроме того, изменение методов атак хакеров определяет необходимость регулярного пересмотра используемых банком элементов системы информационной безопасности и внутрибанковских инструкций и процедур по их применению.

Банк в рамках управления операционным риском при оказании услуг интернет-банкинга должен гарантировать клиенту следующее: устанавливая соединение с определенным банком, клиент направляет информацию именно данному банку, а не мошеннику, организовавшему перенаправление данных;

– данные, направленные в банк, не будут изменены при пересылке;

– информация о клиенте и его операциях не будет раскрыта третьим лицам;

– отправитель данных в адрес клиента может быть однозначно идентифицирован.

При дистанционном обслуживании через Интернет для банков затруднена идентификация клиентов, отсутствуют личный контакт и контроль со стороны сотрудников банка как в момент открытия счета, так и при последующем проведении операций. Таким образом, оказывается неэффективным один из обязательных механизмов внутреннего контроля, и, соответственно, банки должны адаптировать процесс мониторинга трансакции с учетом произошедших изменений в технологии проведения операции. Высокий уровень рисков банковской деятельности позволяет рассматривать технологии в качестве самостоятельного объекта контроля.

Правовой риск. Уровень правового риска, зависит в первую очередь, от степени проработанности законодательства по вопросу интернет-банкинга. Во многих странах действуют законы об электронной подписи, позволяющие подвести правовую базу под осуществление электронной коммерции в целом и интернет-банкинга в частности. Например, наличие в правовой системе Федерального закона от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи» позволяет существенно снизить правовой риск, связанный с интернет-банкингом. Банк, занимающийся интернет-банкингом, будет подвергаться правовому риску и в случае несанкционированного распространения или утечки частной информации клиентов.

Специфика интернет-банкинга вносит определенные проблемы и в управление рисками.

1. В сфере технологии и обслуживания клиентов через Интернет широко используются инновации. Банки, испытывая давление со стороны конкурентов, вводят новые операционные прикладные программы в сжатые сроки. Иногда с момента разработки концепции услуги до ее внедрения проходит всего несколько месяцев. Эта тенденция к экспромту мешает своевременному проведению адекватной стратегической оценки и анализа степени риска, проверки безопасности новой высокотехнологичной услуги.

2.Системы интернет-банкинга и связанные с ним прикладные программы, как правило, интегрируются с компьютерными системами банка для обеспечения прямой сквозной обработки электронных трансакций. И хотя при этом снижаются возможности субъективной ошибки и мошенничества, которые характерны для ручной обработки данных, одновременно увеличивается зависимость банков от надежности структуры и архитектуры систем, равно как и от их операционной совместимости и масштабности.

3.Интернет-банкинг увеличивает и зависимость банков от информационных технологий, приводя к росту проблем безопасности и к технической сложности операций. В целях обслуживания информационных систем банк стремится к установлению тесного партнерства с третьими сторонами – такими небанковскими организациями, как интернет-провайдеры, телекоммуникационные компании и другие технологические фирмы, которые находятся вне сферы банковского регулирования и надзора.

4.Интернет – открытая сеть, доступная из любой точки земного шара для любых организаций или частных лиц, с маршрутами передачи сообщений через различные серверы, разбросанные по всему миру посредством беспроводных средств.

Глобальный характер Интернета существенным образом увеличивает важность и вместе с тем сложность систем контроля за обеспечением безопасности, методов аутентификации клиентов, защиты данных и норм соблюдения клиентской тайны. Поэтому традиционные принципы управления рисками банковской

деятельности должны учитывать сложные характерные особенности интернет-услуг. Банкам целесообразно использовать интегрированный подход к управлению риском, контроль которого должен стать неотъемлемой частью общей структуры управления рисками банка. Необходимо разрабатывать процедуры управления, соответствующие специфике интернет-услуг, общему профилю риска, операционной структуре и корпоративной культуре управления. Системы контроля и безопасности банка должны быть адекватными технологическим нововведениям.

Принципы управления рисками интернет-банкинга были впервые сформулированы Базельским комитетом по банковскому надзору в 2003 г. в документе, получившем соответствующее название «Принципы управления рисками для предоставления банковских услуг в электронной форме». Следует отметить, что комитет не определяет документ как абсолютное требование или даже описание «наилучших решений» для банков, поскольку установка детальных требований к управлению рисками в сфере электронного банкинга может оказаться неблагоприятным фактором ввиду того, что они могут быстро устареть из-за скорости изменений, связанных с технологическими инновациями и видами услуг. Поэтому принципы управления рисками, сформулированные Базельским комитетом, являются, скорее, рекомендациями для кредитных организаций, осуществляющих интернет-банкинг, в области построения надлежащей системы безопасности применения интернет-технологий.

Принципы управления рисками интернет-банкинга классифицируются на три группы:

- для совета директоров и правления банка;
- для выбора и адекватного функционирования средств обеспечения безопасности;
- для повышения значимости управления правовым и репутационным рисками.

Такое деление не случайно и предопределяется иерархией приоритетов в области управления рисками. Первые три принципа управления рисками электронного банкинга сгруппированы в разделе «Наблюдение со стороны совета и руководства».

Группа принципов «Наблюдение со стороны совета и руководства» включает:

1. Эффективное наблюдение со стороны руководства за деятельностью в рамках электронного банкинга.

2. Организацию полноценного процесса контроля за безопасностью.

3. Организацию полноценного и непрерывного процесса наблюдения за выполнением обязательств и управлением отношений банка с провайдерами услуг и прочими организациями, обеспечивающими поддержку выполнения операций интернет-банкинга.

Их суть заключается в том, что совет директоров и правление банка отвечают за разработку корпоративной стратегии банка и за организацию эффективного наблюдения за рисками. Предполагается, что они принимают четкие, обоснованные и формализованные стратегические решения относительно того, будет ли в будущем предоставлять банк услуги в рамках интернет-банкинга, и если да, то каким именно образом.

Совет директоров несет ответственность за политику управления рисками при осуществлении операций интернет-банкинга и за наличие контроля за безопасностью. В свою очередь, правление банка должно обеспечить надлежащее содержание этих процессов. Это означает введение должных правил авторизации и способов аутентификации, средств контроля логического и физического доступа, построение адекватной структуры безопасности для поддержания необходимых допусков и ограничений в части действий как внутренних, так и внешних пользователей, а также целостности трансакций, записей и информации.

Следующие семь принципов управления рисками Базельским комитетом сгруппированы в тематическую категорию «Средства обеспечения безопасности»:

1. Аутентификация клиентов в операциях интернет-банкинга.

2. Отсутствие отказов от проведения операций и возможность учета для трансакций, осуществляемых в рамках интернет-банкинга. Данный принцип управления рисками интернет-банкинга означает,

что банкам следует использовать те методы аутентификации трансакций, которые способствуют невозможности отказа от операций (доказательного подтверждения операции) и обеспечивают возможность учета трансакций в рамках интернет-банкинга.

3. Должные меры по обеспечению разделения обязанностей.

4. Средства авторизации в системах электронного банкинга, базах данных и прикладных программах.

5. Целостность данных в трансакциях электронного банкинга, записях и информаци.

6. Организация формирования точных аудиторских записей для трансакций, осуществляемых в рамках электронного банкинга.

7. Конфиденциальность банковской информации.

Меры, принимаемые для сохранения конфиденциальности, должны быть соразмерны значимости переда ваемой и/или хранимой в базах данных информации.

Такая категория представляет особую значимость вследствие повышенной сложности технологий, применяемых при операциях интернет-банкинга. Поэтому для банка актуальны вопросы аутентификации клиентов, целостности данных и трансакций, разделения обязанностей, использования средств управления авторизацией, поддержания аудиторских записей, а также конфиденциальности банковской информации.

Третья группа принципов управления рисками электронного банкинга включает рекомендации по управлению правовым и репутационным рисками. Их возможное обострение обусловлено различиями в законодательных актах стран, через которые производятся такого рода операции, в обеспечении конфиденциальности информации и правилах защиты клиента, действующих на территориях этих стран.

Банки несут ответственность за обеспечение требований раскрытия информации, защиты клиентских данных и доступности деловых операций, а также требований, действующих при проведении операций через традиционные каналы предоставления банковских услуг. В этой связи Базельский комитет по банковскому надзору формулирует еще четыре принципа управления рисками, которым

рекомендуется следовать банкам, оказывающим услуги интернет-банкинга.

Группа принципов «Усиление контроля правовых и репутационных рисков» включает:

1. Достоверность и полноту раскрытия информации для обслуживания в рамках электронного банкинга.

2. Конфиденциальность информации о клиентах.

3. Планирование производительности, непрерывности операций и на случай непредвиденных обстоятельств для обеспечения доступности систем и обслуживания в рамках интернет-банкинга.

4. Планирование реагирования на непредвиденные события.

Базельские принципы являются опорными пунктами выстраивания комплексной системы управления рисками интернет-банкинга, без которых вся последующая работа банка по идентификации, анализу, оценке и минимизации рисков утрачивает смысл.

Рекомендации Базельского комитета по банковскому надзору были учтены и Банком России при разработке принципов управления рисками интернет-банкинга для российских банков, которые имеют рекомендательный характер.

В рекомендациях Банка России по организации управления рисками, возникающими при осуществлении операций с применением систем интернет-банкинга, подчеркивается, что обеспечение эффективного управления ими является одной из целей внутреннего контроля. Согласно этим рекомендациям, оптимальная модель управления рисками в данной сфере должна включать следующие компоненты:

• квалифицированная политика информатизации, в том числе внедрения и развития технологий интернет-банкинга, проводимая руководством кредитной организации и обеспечивающая полнофункциональность системы – выполнение предполагающихся функций банковского обслуживания;

• тщательно продуманная архитектура автоматизированной банковской системы;

• адекватные меры по обеспечению информационной безопасности по всему информационному контуру интернет-

банкинга, гарантирующие доступность и непрерывность банковского обслуживания, а также защиту информации от несанкционированного доступа, модификации либо уничтожения;

• организация внутрибанковских процессов и процедур, соответствующих масштабу, технологической и технической сложности предоставляемого обслуживания клиентов посредством интернет-банкинга;

• отлаженная система внутреннего контроля, охватывающая всю технологическую цепочку интернет-банкинга и организационную структуру, начиная с руководства банка;

• эффективная система финансового мониторинга, оказывающая противодействие попыткам использования системы интернет-банкинга в противоправных целях;

• содержательное и всеобъемлющее организационное, информационное, методическое и консультационное обеспечение клиентов;

• оптимальные, с точки зрения минимизации сопутствующих рисков, взаимоотношения кредитной организации со своими провайдерами и вендорами.

• Рекомендации Банка России учитывают и трансграничный характер услуг интернет-банкинга. Так, банкам рекомендуется выявлять возможные дополнительные источники рисков, возникающих в связи с нарушением законодательства зарубежных государств или территорий, а также дополнительные факторы рисков, относящихся к иным юрисдикциям, в том числе к соблюдению рекомендаций ФАТФ4 (FATF 40 Recomme№datio№s). Соблюдение основного постулата организации риск-ориентированной системы контроля, а именно ее независимости от бизнес-процессов, будет способствовать минимизации рисков интернет-банкинга.

Особенности интернет-банкинга требуют применения более гибких и динамичных подходов надзора, способных постоянно модифицироваться с учетом быстро происходящих изменений в среде информационных технологий.

Таким образом, новые электронные технологии помогают банкам изменить взаимоотношения с клиентами и найти новые

средства для извлечения прибыли. Банковские компьютерные системы на сегодняшний день являются одной из самых быстро развивающихся областей прикладного сетевого программного обеспечения.

2.3. Перспективные методы обеспечения безопасности электронных платежей

На сегодняшний день банки предлагают достаточно широкий спектр услуг, объединенных общим термином – дистанционное банковское обслуживание (ДБО).

С точки зрения способов оказания услуг ДБО выделяют следующие виды:

- интернет-банкинг,
- мобильный банкинг,
- внешние сервисы (с использованием киосков, банкоматов, АТМ),
- телефонный банкинг – услуги ДБО на основе банковской системы голосовых сообщений,
- классический банк-клиент.

В последнее время хищения денежных средств через системы ДБО стали острой проблемой для большинства банков и их клиентов. В финансово-кредитных организациях, имеющих развитую систему ДБО, фиксируется от 6 до 8 попыток проникновения в системы ДБО в неделю. При этом убытки от противоправных действий киберпреступников в рамках ДБО в среднем для одного банка составляют около 10 млн рублей в год, и эти суммы увеличиваются из года в год. Так, по данным Центрального банка России, в 2014 году отмечался двукратный рост числа зарегистрированных краж денежных средств из систем ДБО.

Очевидно, что с развитием рынка услуг ДБО все большее значение приобретают вопросы, связанные с появлением новых видов банковских рисков и применением адекватных мер безопасности электронных услуг для банка и клиента. Одним из факторов риска в

системе защиты ДБО является сложность обеспечения доверенной среды исполнения на стороне пользователя[1].

Наиболее распространенным средством аутентификации пользователей были пароли, и первая волна вредоносного программного обеспечения (ПО) была направлена именно на кражу паролей.

Криптографические ключи и сертификаты, если они не были защищены специальными аппаратными устройствами: токенами, смарт-картами, – также стали легкой «добычей» при использовании вредоносного ПО типа «троянский конь». Конечно, существуют способы защиты от подобных атак, например, своевременная установка обновлений операционной системы (ОС) и ПО на стороне клиента банка, применение антивирусного ПО или персонального межсетевого экрана со средствами обнаружения вторжений и т.п. Да и просто – ответственное поведение пользователя – отказ от посещения сайтов с «плохой репутацией» и загрузки ПО из непроверенных источников. Но большая часть пользователей пренебрегает этими мерами предосторожности.

Кроме того, 0-day-уязвимости в ОС и прикладном ПО, прежде всего в java-машинах, flash-плеерах, плагинах браузеров, ПО Acrobat Reader и др., сейчас активно эксплуатируются киберпреступниками для проведения поэтапных атак на пользователей ДБО. Поиск 0-day-уязвимостей и создание на их основе вредоносного ПО, например с функциями «троянский конь» или для обхода антивирусных программ, взлома популярных веб ресурсов и размещения на их страницах ссылок (iframe) с «плохим» ПО, используемым в дальнейшем для осуществления нападения на компьютер жертвы, – это отдельный бизнес. Можно приобрести любые, нужные для осуществления киберпреступления, софт и услуги[2].

Одна из защитных мер была известна давно –это аппаратное устройство для защиты криптографических ключей –смарт-карта или

[1] Мокрушина А.Л., Рустамова Э.О. Интернет-банкинг - новая форма старых услуг: понятие, безопасность, перспективы развития системы // Проблемы и перспективы развития современного законодательства: сборник материалов межкафедральной научно-практической конференции юридического факультета Российской таможенной академии. М.: Изд-во Рос. тамож. акад., 2013. С. 63-66.

[2] Там же.

токен. Другая – одноразовые пароли, которые выдаются в банкомате, печатаются на скретч-карте или высылаются с помощью SMS на мобильный телефон клиента.

Каждая значимая банковская операция подтверждается новым одноразовым паролем. Однако и эти средства защиты были взломаны –атаки типа «человек посередине» и фишинговые методы также активно используются мошенниками для обхода одноразовых паролей.

«Человек посередине» – это метод компрометации канала связи, при котором взломщик, подключившись к каналу между контрагентами, осуществляет активное вмешательство в протоколы передачи, удаляя, искажая информацию или навязывая ложную.

В случае фишинга схема действий такова: клиент заманивается на фишинговый сайт, внешне очень похожий на сайт реального банка с системой ДБО. «Сайт-злоумышленник» предлагает точно такую же последовательность действий, как и легитимный – запрашивает пароль, позволяет сформировать банковскую операцию, а потом запрашивает одноразовый пароль на совершение этой операции. Пользователь вводит необходимые данные, и, таким образом, пароли становятся доступны кибермошенникам, которые используют их для манипуляции со счетом жертвы и хищения денежных средств.

Эффективные средства защиты – одноразовые пароли, формируемые на основании информации о транзакции, или криптографические USB-токены. Настоящим ударом по безопасности систем ДБО стала атака «человек в браузере». Этот тип «троянской программы» применяется в тех случаях, когда криптографические ключи хранятся на токене и их нельзя украсть. Но можно «подсунуть» на подпись пользователю поддельное платежное поручение, а на экране компьютера клиента банка отобразить (с помощью вредоносного ПО) действительно сформированное пользователем платежное поручение. Весь процесс проходит скрытно, без каких-либо очевидных признаков для пользователя.

Средством защиты от «человека в браузере» может стать считыватель смарт-карт с возможностью визуального контроля подписываемого документа. Устройство позволяет показать клиенту в

«защищенной среде» – на экране смарт-карты – номер счета, куда будет переведен его платеж, в надежде, что пользователь сравнит длинную последовательность цифр с той, что на экране компьютера. Увы, практика показывает, что не все пользователи применяют этот метод.

Для предупреждения подобных атак необходима система противодействия как внешнему, так и внутреннему мошенничеству, так называемые решения антифрод, работающие в реальном времени. Другими словами, это комплекс организационных и технических мер, обеспечивающих дополнительную защиту автоматизированных банковских систем и систем дистанционного банковского обслуживания.

Такие системы содержат наборы правил, позволяющие с высокой долей вероятности обнаружить транзакции, сформированные мошенниками. Это, например, «черные» и «белые» списки. В «черные» списки попадают те получатели платежей, которые уже были уличены в участии в мошеннических схемах, в «белые» – те, которым клиент платил и не обжаловал этот платеж. При анализе могут быть использованы, например, данные геотаргетинга – для обнаружения ситуаций, когда один и тот же пользователь работает почти одновременно из разных стран. Или система слежения за бот-сетью – сетью из «компьютеров-зомби», способных выполнять несанкционированные легальными пользователями действия (похищать данные, осуществлять рассылки спама, проводить атаки отказа в обслуживании и т.д.)[1].

Возможно также создание профиля пользователя, учитывающего различные параметры выполняемых операций: запрашиваемую сумму, дату и время, географию – и определяющего уровень риск для каждой транзакции по этому профилю. Транзакции с высоким уровнем рисков можно запрещать или ограничивать по сумме, или требовать дополнительной авторизация для выполнения операции[2].

[1] Корякин В.М., Саенко А.Ю. Некоторые вопросы безопасности использования банковских карт // Право в вооруженных силах. 2012. № 2. С. 75.
[2] Мокрушина А.Л., Рустамова Э.О. Указ. соч.

В комплексе с программно-аппаратными средствами противодействия компания «АСТ» применяет методику оценки защищенности системы ДБО. «АСТ» как аудитор систем ДБО осуществляет следующие виды технологических аудитов:

1. Аудит внешнего периметра – проверки правил фильтрации, типовых конфигураций сервисов, тестирование на известные удаленные уязвимости в ОС и сервисах.
2. Аудит архитектуры системы – проверки парольной политики, ролей пользователей, правил логики системы.
3. Аудит защищенности web-приложений – поиск известных и новых уязвимостей в приложениях.
4. Проверки на наличие скрытых скриптов и шифрования web-соединений.
5. Аудит защищенности на уровне СУБД – контроль парольной политики СУБД, проверки на уязвимости и ошибки конфигурации, шифрование критичных данных и др.
6. Аудит защищенности клиентской части системы – поиск уязвимостей, анализ работы клиента с криптографией, проверка настроек и конфигураций клиентского ПО, системы хранения паролей на клиентской части и др.

По результатам проведенных проверок и выявленных уязвимостей определяются возможные векторы атак как на клиентов системы, так и на серверы ДБО.

Снижение рисков мошенничества в системах ДБО за счет дополнительного анализа типового поведения клиентов, анализа аномального поведения и введение дополнительных проверок позволяют снизить прямые финансовые потери банков, связанные с мошенничеством, повысить репутацию и уровень доверия к банку в глазах клиентов, инвесторов и партнеров.

Информационную безопасность в банке обеспечивает управление информационной и экономической безопасности Департамента банковской безопасности.

В рамках обеспечения информационной безопасности управление выполняет следующие функции:

1. Разрабатывает основные направления использования в

банке программных и программно-технических средств защиты информации с ограниченным доступом (ИСОД), учета, хранения ключевой информации и документов в подразделениях и филиалах банка.

2. Проводит анализ и организовывает работу по выявлению возможных каналов утечки ИСОД.

3. Осуществляет сбор и анализ информации о перспективных программных и программно-технических средствах защиты информации с учетом требований Центрального банка РФ и соответствующих нормативных и законодательных документов РФ, а также вносит предложения относительно их внедрения в учреждениях банка.

4. Оказывает методическую и практическую помощь структурным подразделениям банка по вопросам защиты ИСОД в системе электронных платежей, электронного документооборота, программных и программно-технических комплексах, телекоммуникационных системах.

5. Принимает участие в подготовке технических заданий, тестировании программных комплексов и систем, в которых обрабатывается ИСОД, проведении экспертизы на предмет их защищенности от несанкционированного доступа, модификации и фальсификации.

6. Предоставляет свои предложения относительно их совершенствования.

7. Контролирует порядок использования, учета и хранения средств защиты, ИСОД в подразделениях и филиалах банка, а также выполняет требования информационной безопасности в корпоративных (локальных) сетях банка, системе электронных межбанковских переводов (СЭМП), внутренних платежных системах (ВПС), системе автоматизации банка (САБ), интегрированной банковской системе (ИБС), электронной почте, центральном информационном и промышленном хранилище данных, Интернете, системах электронного документооборота.

8. Проводит проверки эффективности внедренных мероприятий в сфере информационной безопасности и осведомленности пользователей в вопросах информационной безопасности; согласовывает предоставление доступа пользователям к работе с соответствующими

системами, сетями, базами данных, к хранилищам, где обрабатывается информация, которая содержит банковскую или коммерческую тайну.

9. Осуществляет мониторинг инцидентов в отрасли информационной безопасности (фиксация попыток несанкционированных действий с системами);

10. На основании запросов клиентов, банков-корреспондентов или по поручению руководства банка проводит служебные расследования по фактам нарушения правил работы с электронными платежными документами, режима и др., предоставляет соответствующие рекомендации и предложения относительно устранения обнаруженных недостатков.

11. Взаимодействует с компетентными органами по вопросам несанкционированных действий на электронные платежные документы и внешних попыток атак на корпоративную сеть банка; выполняет генерацию реальных ключевых данных для защищенных программных и программно-технических комплексов и систем банка, осуществляет их сертификацию и учет.

12. Осуществляет контроль соблюдения режима в помещениях с ограниченным доступом и ведет электронные архивы ключевой информации.

13. Эксплуатирует многоуровневые системы управления центрами распределения и сертификации ключей, которые используются в работе с защищенными системами, программными и программно-техническими комплексами банка.

14. Проводит обучение и инструктажи пользователей программных комплексов и систем, в которых используются средства защиты информации, относительно вопросов выполнения требований информационной безопасности.

15. Согласовывает назначение и проводит учебу (семинары) специалистов по вопросам защиты информации (администраторов защиты информации) банка.

Возглавляет управление начальник управления информационной и экономической безопасности Департамента банковской безопасности.

Выделяют три типа организационных структур управления службы безопасности. Первый тип (рис. 6) исходит из отказа от услуг специализированных структур в лице частных охранных агентств или службы вневедомственной охраны Министерства внутренних дел. Данный используется традиционно крупными банками, реализующими стратегию упреждающего противодействия.

Рис. 6. Типовая структура департамента безопасности банка, не использующего услуги специализированных структур

Второй подход основан на передачу в аутсорсинг функций обеспечения безопасности банка на контрактной основе. Преимуществами данного подхода выступают: сокращение капиталоемкости, профессионализм привлеченных сотрудников, отсутствие ряда ограничений, обусловленных правилами ведения частной охранной деятельности. Недостатком данного подхода выступает низкий уровень доверия к внешним структурам. Данный подход используется банками с государственным участием или региональными банками (рис. 7), реализующими пассивную стратегию развития.

Рис. 7. Типовая структура департамента безопасности банка, использующего услуги специализированных структур

Третий подход основан на привлечении специализированных частных структур для решения отдельных задач.

При организации эффективной системы безопасности банковской деятельности необходимо придерживаться таких принципов:

комплексность - обеспечение безопасности персонала, материальных и финансовых ресурсов от возможных угроз всеми доступными законными средствами, методами; обеспечение безопасности информационных ресурсов в течение всего жизненного цикла, на всех технологических этапах их обработки и использования, во всех режимах функционирования; возможность системы к развитию и усовершенствованию в соответствии с изменениями условий функционирования субъекта;

своевременность - предупредительный характер мероприятий относительно обеспечения безопасности. Постановка заданий, формирования комплексной безопасности на предыдущих стадиях разработки системы безопасности на основании анализа и прогнозирования обстоятельств, угроз безопасности, а также разработка эффективных мероприятий предупреждения;

непрерывность - использование преступниками законных и незаконных методов с целью борьбы с методами защиты, что обеспечивают безопасность деятельности;

активность - защита интересов банковских учреждений путем использования стандартных и нестандартных методов;

законность - система безопасности на основе законодательной базы, которая регулирует процесс осуществления банковской деятельности;

обоснованность - мероприятия и средства защиты, которые должны реализовываться на современном уровне развития безопасности и отвечать установленным требованиям и нормам;

экономическая целесообразность - сопоставление возможных убытков и расходов на обеспечение безопасности (критерий эффективности - стоимость);

специализация - привлечение к разработке и внедрению мероприятий и средств защиты специализированных подразделений или учреждений;

взаимодействие и координация - осуществление мероприятий обеспечения безопасности на основе четкого взаимодействия всех заинтересованных подразделений и служб, посторонних специализированных учреждений; усовершенствование мероприятий и средств защиты на основе собственного опыта, новых технических средств с учетом изменения методов и средств разведки, схем отмывания денег, финансирования терроризма и финансового шпионажа;

централизация управления - самостоятельное функционирование системы безопасности по организационным, функциональным и методологическим принципам с централизованным управлением системой безопасности.

На рис. 8 представлены процессы, которые делегируются различным структурным подразделениям банка в рамках формирования действенной системы безопасности банковской организации.

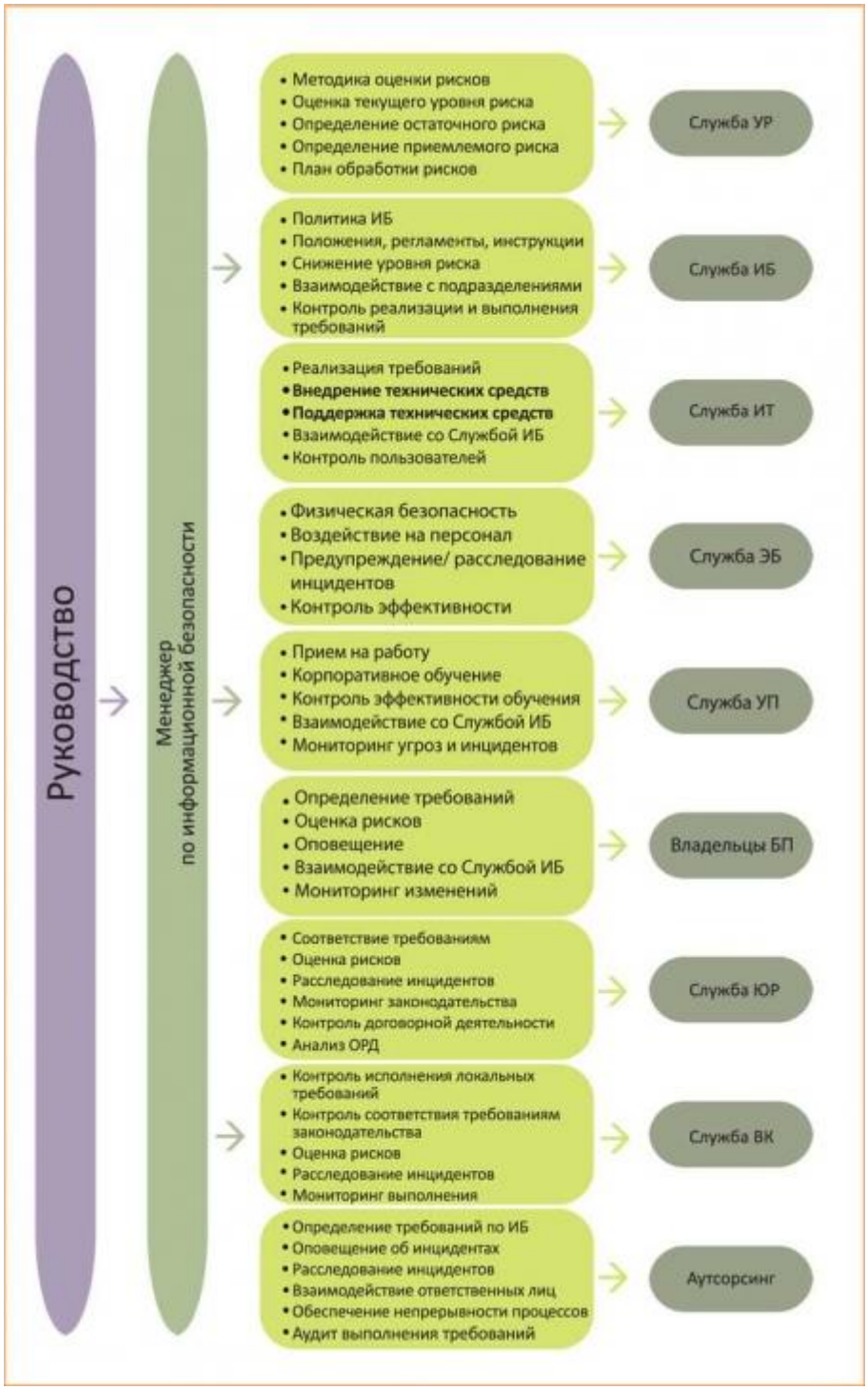

Рис. 8. Реализация стратегии обеспечения банковской безопасности

Где Служба ВК – служба внутреннего контроля
Служба ЮР – юридическая служба
Владельцы БП – владельцы бизнес-процессов
Служба УП – служба управления персоналом
Служба ЭБ – служба экономической безопасности

Служба Ит – служба информационных технологий

Служба ИБ – служба информационной безопасности

Служба УР – служба управления рисками

Основной целью системы безопасности банков является предупреждение убытков от разглашения конфиденциальной информации; кражи финансовых и материально-технических ценностей, нарушения функционирования информационных систем. Таким образом, целями системы безопасности банковской деятельности должны быть: защита прав банковских учреждений, их структурных подразделений и сотрудников; сохранение и эффективное использование финансовых, материальных, информационных ресурсов; повышение конкурентоспособности и рост прибыльности за счет обеспечения качества банковских услуг и безопасности для клиентской базы.

ЗАКЛЮЧЕНИЕ

Совершенствование системы банковской деятельности предполагает совершенствование институциональной базы банковской системы на основе пакета законов, предусматривающих ужесточение требований к системам страхования рисков по различным видам деятельности кредитных учреждений и степени взаимной согласованности этих систем внутри отдельного банка (стандарты Базельского соглашения). Таким образом, одной из актуальных задач современной России становится задача обеспечения экономической безопасности в кредитно-банковской системе.

В ходе исследования были выявлены основные угрозы безопасности в банковской сфере:

• развитие и совершенствование технологий и методов современных атак;

• сложность и комплексность требований законодательства, нормативных документов регуляторов, требований международных платежных систем;

• утечки банковской тайны, защита от «инсайдеров»;

• сложность автоматизированной банковской системы, проблемы управления доступом к данным;

• взаимодействие с сетью общего пользования Интернет;

• необходимость создания нормативной базы по электронному банкингу.

В составе существующих угроз выявлены:

1. Прямые финансовые потери — взлом внешними злоумышленниками систем дистанционного банковского обслуживания, кража денежных средств у клиентов банка.

2. Репутационные риски — нарушение функционирования или взлом публичных банковских сервисов (веб-сайт банка, система электронной почты).

3. Утечка конфиденциальной информации (банковская тайна, персональные данные) — использование уязвимостей веб-браузеров и заражение вредоносным кодом рабочих станций сотрудников банка.

Целью формирования системы безопасности банковской деятельности выступает обеспечение устойчивого функционирования банка и предотвращение внутренних и внешних угроз, что предусматривает решение следующих задач: защита его законных интересов от противоправных посягательств, безопасность и охрана здоровья персонала, недопущение хищения финансовых и материальных средств, порча и уничтожение имущества, ценностей, разглашение коммерческой тайны, утечки и несанкционированного доступа к служебной информации, нарушения работы технических средств, обеспечивающих банковскую деятельность.

Система безопасности банка включает ряд подсистем:

1. Правовую, наличие которой формирует правовую обеспеченность или состояние при котором все аспекты функционирования системы управления безопасностью регламентированы законодательными актами и соответствующими нормативными документами. Она включает правовую культуру, права и обязанности должностных лиц, правовое регулирование отношений людей в рабочих коллективах, между различными командными инстанциями, между начальниками и подчиненными и т.д.

2. Организационную, или построение и устойчивое функционирование системы управления безопасностью на различных уровнях; развитие и создание оптимальной организационно-штатной структуры; организационные и другие документы, регламентирующие функционирование системы безопасности банка, организация управления безопасностью повседневной деятельности и т.д.

3. Техническую политику в оснащении банка современными средствами безопасности, подбор квалифицированных технических специалистов, высокие требования к техническим средствам системы безопасности, всестороннее обеспечение системы безопасности тех-

ническими средствами, диагностика, осмотр, обслуживание технических средств и т.д.

4. Психологический анализ управления безопасностью, учет психологических факторов в работе банковских служащих в повседневной деятельности и, особенно, в экстремальных ситуациях, психологическая подготовка банковских служащих, отвечающая требованиям данного вида деятельности и способствующая эффективному выполнению своих служебных обязанностей и т.д.

В государственной стратегии России, реализуемой в условиях международной интеграции и глобализации, можно выделить три важнейших аспекта, способствующих модернизации банковского сектора экономики: национальные экономические интересы, отвечающие требованиям экономической безопасности; профилактика и пресечение угроз экономической безопасности; диверсификация экономической политики в сфере безопасности. Таким образом, комплексное применение банковских инноваций, инфокоммуникационных технологий и традиционных подходов существенно повысит эффективность, приведет к персонализации и дифференциации финансовых процессов в кредитных организациях, позволит расширить клиентскую базу, создавая условия для совершенствования коммуникативной компетенции и кредитного посредничества, необходимых для развития банковской сервисной системы. Решение этих и других задач способствует обеспечению экономической безопасности банковской деятельности на разных уровнях.

СПИСОК ЛИТЕРАТУРЫ

Нормативные правовые акты

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 ; с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ // Собрание законодательства РФ. – 2014. – № 31. – Ст. 4398.
2. О банках и банковской деятельности : Федеральный закон от 2 декабря 1990 г. № 395-I // Ведомости съезда народных депутатов РСФСР. – 1990. – № 27. – Ст. 357.
3. О несостоятельности (банкротстве) кредитных организаций : Федеральный закон от 25 февраля 1999 г. № 40-ФЗ// Собрание законодательства Российской Федерации. – 1999. – № 9. – Ст. 1097.
4. О Центральном банке Российской Федерации (Банке России) : Федеральный закон от 10 июля 2002 г. № 86-ФЗ // Собрание законодательства Российской Федерации. – 2002. – № 28. – Ст. 2790.
5. О страховании вкладов физических лиц в банках Российской Федерации : Федеральный закон от 23 декабря 2003 г. № 177-ФЗ // Собрание законодательства Российской Федерации. – 2003. – № 52 (часть I). – Ст. 5029.
6. О полиции: Федеральный закон от 07.02.2011 № 3-ФЗ : ред. от 18.06.2017 // Официальный интернет-портал правовой информации. – Режим доступа : http://www.pravo.gov.ru, 18.06.2017, № 0001201706180007.
7. О национальной платежной системе : Федеральный закон от 25.12.2012 №267-ФЗ : ред. от 18.07.2017 // Официальный интернет-

портал правовой информации. – Режим доступа : http://www.pravo.gov.ru, 19.07.2017, № 0001201707190012.

8. Об оперативно-розыскной деятельности : Федеральный закон от 12 августа 1995 г. № 144-ФЗ : в ред. от 06.07.2016 // Официальный интернет-портал правовой информации. – Режим доступа : http://www.pravo.gov.ru, 07.07.2016, № 0001201607070016.

9. О персональных данных: Федеральный закон от 27.07.2006 № 152-ФЗ // Официальный интернет-портал правовой информации. – Режим доступа : http://www.pravo.gov.ru.

10. О частной детективной и охранной деятельности: закон РФ от 11 марта 1992 г. 2487-I в ред. от 03.07.2016 // Официальный интернет-портал правовой информации – Режим доступа : http://www.pravo.gov.ru, 03.07.2016, № 0001201607030004

11. О Стратегии национальной безопасности Российской Федерации : указ Президента Российской Федерации от 31 декабря 2015 года № 683. – Режим доступа : https://rg.ru/2015/12/31/№ac-bezopas№ost-site-dok.html. (дата обращения 20.07.2017).

12. Концепция долгосрочного социально-экономического развития Российской Федерации на период до 2020 года [Электронный ресурс]: утв. распоряжением Правительства РФ от 17 нояб. 2008 г. № 1662-р. – Режим доступа:: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=law;n=90601 (дата обращения : 20.07.2017).

13. Доктрина информационной безопасности Российской Федерации: утверждена Президентом Российской Федерации 9 сентября 2000 г. № Пр – 1895.

14. Порядок обеспечения и защиты банковской информации : положение ЦБ РФ от 16.12.2003 г. № 242-П.

15. 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 : положение Банка России от 9 июня 2012 года № 382-П (в ред. указания Банка России от 5 июня 2013 года № 3007-У).

16. Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных : приказ Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 года № 21.

17. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения : стандарт Банка России СТО БР ИББС -1.0. – 2010.

18. О Стратегии развития банковского сектора Российской Федерации на период до 2015 года : заявление Правительства РФ и ЦБР от 5 апреля 2011 г. №№ 1472п-П13, 01-001/1280. – Система ГАРАНТ. – Режим доступа : http://base.garant.ru/591345/#ixzz3unoqGaTJ.

Специальная литература

1. Акимов В. Оценка и прогноз стратегических рисков : теория и практика / В. Акимов // Право и безопасность. – 2014. – № 1.

2. Щербакова Г. Анализ и оценка банковской деятельности (на основе отчетности, составляемой по российским и международным стандартам) / Г. Щербакова. – М. : Вершина, 2012.

3. Архипов А. Экономическая безопасность: оценки проблемы, способы обеспечения / А. Архипов, А. Городецкий, Б. Михайлов // Вопросы экономики. – 2014. – № 12.

4. Атаманов Г.А. Методология безопасности / Г.А. Атаманов // Фонд содействия научным исследованиям проблем безопасности «Наука-XXI». – 2011. – Режим доступа: www.Naukaxxi.ru/materials/ 302.

5. Безопасность современного банка. – Режим доступа: http://www.lawmix.ru/bux/52153.

6. Богута Н. Интернет-банкинг : преимущества и недостатки онлайн-систем отечественных банков / Н. Богута. – Режим доступа: Prostobiz.ua (дата обращения: 20.07.2017).

7. Бочаров О.А. Формирование основ экономической безопасности банковской деятельности : автореф. дис. … канд экон. наук / О.А. Бочаров. – М., 2013.

8. Вечканов Г.С. Экономическая безопасность / Г.С. Вечканов. – СПб. : Вектор, 2013.

9. Викулин А. Работа коммерческого банка по предотвращению легализации (отмывания) доходов, полученных незаконным путем / А.Викулин //Банковское дело. – 2014. – № 1.

10. Гамза В.А. Концепция и система безопасности банка / В.А. Гамаза, И.Б. Ткачук. – Шумилова И.И., 2013.

11. Гамза В.А. Безопсность банковсой деятельности / В.А. Гамза, И.Б. Ткачук, И.М. Жилкин. – М. : Юрайт, 2014. – 513 с.

12. Ильясов С. Совершенствование государственного регулирования банковской деятельности // Аналитический банковский журнал. 2013. № 2.

ИТ в банковской сфере. – Режим доступа:http://www.tradinginforex.ru/trade (дата обращения : 20.07.2017).

13. Кирюшин А.В. Правовые аспекты обеспечения экономической безопасности Российской Федерации / А.В. Кирюшин, С.В. Плотников // История государства и права. – 2014. – № 9.

14. Ковалев Р.О. Проблемы криминологического обеспечения взаимодействия правоохранительных органов и банковских структур безопасности в предупреждении преступлений в сфере банковской деятельности / Р.О. Ковалев // Восьмые Всероссийские Державинские чтения (Москва, 14 декабря 2012 года): сборник статей : в 7 кн.: проблемы уголовно-процессуального и уголовного права, криминалистики и криминологии. – М. : РПА Минюста России, 2013. – Кн. 5. – С. 126-131.

15. Концепция безопасности коммерческого банка. – Режим доступа: http://www.bre.ru/security/14277.html.

16. Корякин В.М. Некоторые вопросы безопасности использования банковских карт / В.М. Корякин, А.Ю. Саенко // Право в вооруженных силах.– 2012. – № 2.

17. Кочергина Т.Е. Экономическая безопасность / Т.Е. Кочергин. – Ростов-на-Дону : Феникс, 2012.

18. Кошаева Т.О. Вред, причиняемый экономическими преступлениями / Т.О. Кошаева //Журнал российского права. – 2012. – № 8.

19. Ларьков А.Н. Экономическая преступность и уголовный закон / А.Н. Ларьков // Преступность и закон: тезисы конференции. – М., 2012.

20. Лясковский Е.Н. Организационно-методические основы обеспечения экономической безопасности банковской сферы / Е.Н. Лясковский // Проблемы управления рисками в техносфере. – 2009. – № 1(9)-2(10).

21. Михайлов Л.М. Социально-экономическое развитие России в среднесрочной и долгосрочной перспективе : анализ современных программ и концепций / Л.М. Михайлов // Сб. науч. тр. преподавателей МАЭП. – М. : МАЭП, 2014.

22. Мокрушина А.Л. Интернет-банкинг - новая форма старых услуг: понятие, безопасность, перспективы развития системы / А.Л. Мокрушина, Э.О. Рустамова // Проблемы и перспективы развития современного законодательства : сборник материалов межкафедральной научно-практической конференции юридического факультета Российской таможенной академии. – М. : Изд-во Рос. тамож. акад., 2013. – С. 63 – 66.

23. Овсянникова Е.В. Экономическая безопасность в системе национальной безопасности Российской Федерации в условиях глобализации : дис. ... канд. экон. наук / Е.В. Овсянникова. – М. : 2012.

24. Организация системы информационной безопасности в банке. – Режим доступа: http://www.crime-research.ru/library/Tarnav.htm (дата обращения: 20.07.2017).

Официальный сайт компании International Data Corporation (IDC). – Режим доступа : http://idcrussia.com/ru/ (дата обращения: 20.07.2017).

25. Ревенков П.В. Электронный банкинг: риски недостаточного обеспечения информационной безопасности / П.В. Ревенков // Юридическая работа в кредитной организации. М. : Регламент, 2013. – № 3 (37). – С. 35-49.

26. Репин А.В. Экономическая безопасность в банковской сфере : отзыв лицензии / А.В. Репин // Инновационная экономика: материалы междунар. науч. конф. (г. Казань, октябрь 2014 г.). – Казань : Бук, 2014. – С. 58-61.

27. Россия в глобализирующемся мире: Стратегия конкурентоспособности / Российская академия наук, отделение общественных наук, секция экономики ; акад. Д.С. Львов [и др.]. – М. : Наука, 2014.

28. Технология информационного мониторинга. – Режим доступа : http://sibac.itfo/itdex.php/2009-07-01-10-21-16/3843-2012-09-22-14-46-18 (дата обращения: 20.07.2017).

29. Ткачев В.И. Институт несостоятельности (банкротства) как элемент комплекса мер по обеспечению экономической безопасности хозяйствующих субъектов / В.И. Ткачев // Гражданское право. – 2012. – № 6. – С. 13-17.

30. Финансовый мониторинг в банке. – Режим доступа : http://www.kreditspravka.ru/o-bankah/finansovyj-monitoring-v-bankah.html (дата обращения: 20.07.2017).

31. Характеристика угроз безопасности банка. – Режим доступа : http://otherreferats.allbest.ru/ba№k/00012795_0.html (дата обращения: 20.07.2017).

Цифровому банку будущего быть! – Режим доступа : http://www.bps-sberbank.by/online/ru.about.news.201510290841-html (дата обращения: 20.07.2017).

32. Черкасова Е.А. Информационные технологии в банковском деле: учеб. пособие / Е. А. Черкасова, Е. В. Кийкова. – М. : Академия, 2011. – 320 с

33. Чхутиашвили Л.В. Антикоррупционная безопасность коммерческих банков в России / Л.В. Чхутиашвили // Следователь. – 2014. – № 6 (194). – С. 47-48.

34. Юденков Ю.Н. Интернет-технологии в банковском бизнесе: перспективы и риски : учеб.-практ. пособие / Ю.Н. Юденков, Н.А. Тысячникова, И.В. Сандалов, С.Л. Ермаков. – М. : КНОРУС, 2014. – 318 с.

Научное издание

Наиля Рашидовна **Шевко**
Ольга Геннадьевна **Шмелева**
Гульнара Насимовна **Хадиуллина**

Обеспечение экономической безопасности в банковской сфере при использовании инструментов электронного банкинга

Монография

Корректор Н.А. Климанова
Компьютерная верстка Е.В. Зотина

Подписано в печать 07.12.2017 Усл.печ.л. 5,5
Формат 60х84 1/16 Тираж 30

Типография КЮИ МВД России
420108, г. Казань, ул. Магистральная, 3