

ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ КРЕДИТНОЙ ОРГАНИЗАЦИИ: ФАКТОРЫ, УГРОЗЫ, НАПРАВЛЕНИЯ УКРЕПЛЕНИЯ

Сергей Петрович САЗОНОВ^а, Ирина Александровна ЕЗАНГИНА^{б,*}, Роман Сергеевич ЕВСЕЕВ^с

^а доктор экономических наук, профессор, заведующий кафедрой экономики и финансов предприятий, Волгоградский государственный технический университет, Волгоград, Российская Федерация
sazonovsp@mail.ru

^б кандидат экономических наук, доцент кафедры экономики и финансов предприятий, Волгоградский государственный технический университет, Волгоград, Российская Федерация
ezanginaia@gambler.ru

^с студент факультета послевузовского образования, Волгоградский государственный технический университет, Волгоград, Российская Федерация
roman.evseev@mail.ru

* Ответственный автор

История статьи:

Принята 27.07.2016
Принята в доработанном виде
03.08.2016
Одобрена 11.08.2016

УДК 336.713

JEL: G20, G21, O16

Аннотация

Тема. В современном мире главенствующую роль в процессе формирования коммерческих структур и развития рыночных отношений играют кредитные организации, концентрирующие гигантские финансовые потоки. Аккумуляция денежных средств подвергает банки наибольшей опасности. При этом проблема обеспечения экономической безопасности банка является базовой для широкого круга лиц: управленческого звена, персонала, акционеров, клиентов. Проблемы одной финансовой организации могут отразиться на состоянии отрасли в целом, затрагивая все слои населения и оказывая влияние на политику государства.

Цели. Актуализировать понятие «экономическая безопасность», подходы к его определению, опасности, угрозы, методы управления применительно к современному коммерческому банку.

Методология. Инструментарно-методический аппарат работы основан на использовании системно-функционального подхода, в рамках которого применялись общенаучные методы: абстрагирование, анализ, синтез, индукция и дедукция.

Результаты. Доказано, что на уровень безопасности современного банка наряду с традиционными видами рисков, выступающими объектами перманентного управления, воздействуют новые виды угроз, в особенности риск дистанционного банковского обслуживания (ДБО). Идентифицировано понятие «экономическая безопасность банка». Уточнена специфика этого термина, связанная с обеспечением условий для достижения максимального финансового результата.

Применение. Результаты работы могут быть учтены в финансовой политике кредитной организации, особенно в управлении рисками ДБО.

Выводы. Основным методом оценки безопасности кредитной организации выступает индикаторный подход, используемый в управлении традиционными рисками.

В связи с угрозами злоумышленного характера и несанкционированного доступа, реализуемыми через ДБО, необходим комплексный подход к управлению клиентской базой банка для обеспечения конфиденциальности, целостности, аутентичности банковской информации и экономической безопасности.

Ключевые слова:

экономическая безопасность, индикаторный подход, банковский риск, риск ДБО, несанкционированная операция

© Издательский дом ФИНАНСЫ и КРЕДИТ, 2016

Под экономической безопасностью организации понимается возможность эффективного достижения основной ее цели – получения прибыли за счет наиболее рационального выполнения функций в условиях влияния внешних и внутренних угроз.

Экономическая безопасность организаций зависит в первую очередь от способности формировать конкурентные преимущества, которые являются основой стабильной прибыльной деятельности. Следовательно, экономическая безопасность

напрямую тесно связана с экономической эффективностью организации.

С другой стороны, экономическая безопасность включает в себя сохранение финансовой устойчивости, платежеспособности, планирование будущих денежных потоков экономического субъекта, безопасность занятости [1, с. 156]. По этой причине определение оптимального уровня безопасности предприятия часто сводится к расчету известных финансовых показателей

ликвидности, финансовой устойчивости, деловой активности [2, с. 94].

Резюмируя отмеченное, экономическую безопасность предприятия идентифицируем как состояние экономико-правовых отношений, организационных связей, финансовых, материальных, трудовых, информационных ресурсов, гарантирующее стабильность, финансово-экономический успех, инновационное технологическое и общественное развитие.

При исследовании экономической безопасности кредитной организации акценты традиционно смещаются на обеспечение условий, позволяющих ей достичь максимального финансового результата. В этой связи безопасность выступает объектом угроз преступных посягательств и предполагает защищенность банка от угроз внешнего и внутреннего характера, влияния дестабилизирующих факторов. Это позволяет банку сохранить и эффективно использовать свой потенциал [3, с. 16].

Основными видами угроз безопасности банковской деятельности являются:

- угроза потери имущества;
- угроза порядку функционирования;
- угроза операционной деятельности [4, с. 98].

Соответственно, управление экономической безопасностью коммерческого банка включает в себя совокупность методов и приемов, с помощью которых обеспечивается его способность избегать угроз экономического характера, поддерживать суверенность национальной экономики, ее стабильность и устойчивость [5, с. 444].

Таким образом, вопросы обеспечения экономической безопасности предпочтительно рассматриваются в рамках концепции риск-менеджмента, направленного на идентификацию, измерение и уменьшение потенциальных потерь в деятельности коммерческого банка.

В данном контексте все факторы риска для банка могут быть сгруппированы по различным признакам¹. При этом наибольшее распространение получила идентификация опасностей в зависимости от сферы их возникновения, соответственно, на внутренние и внешние [6, с. 365].

¹ Гринько Е.Л., Леонтьева Е.М. Идентификация рисков дистанционного банковского обслуживания // Актуальные проблемы экономики, социологии и права. 2016. № 1. С. 21–24.

Внешние и внутренние риски обусловлены действиями субъектов, регулирующих банковский процесс либо участвующих в нем [7, с. 29]. Внешние факторы включают в себя социально-политическую, общеэкономическую ситуацию, состояние финансового рынка, степень развития банковской системы. Они детализированы на рис. 1.

Совокупность присущих кредитной организации внутренних факторов экономической безопасности проиллюстрирована на рис. 2.

Основное внимание в анализе факторов безопасности хозяйствующего субъекта должно уделяться организации защиты от угроз злоумышленного, несанкционированного доступа к информации, составляющей коммерческую тайну, и от ошибочных действий персонала. Возможность проявления любой опасности должна своевременно распознавать, оценивать и предотвращать служба безопасности банка.

Однако рассмотрение аспектов безопасности, связанных с проявлением реальных и потенциальных угроз только злоумышленного характера, нельзя считать исчерпывающим в силу нескольких причин:

- в числе прочего безопасность коммерческого банка зависит от способности противостоять угрозам, исходящим как из внешней среды, так и со стороны персонала самого учреждения;
- из-за чрезмерной стоимости защитных систем, несоизмеримой с вероятными экономическими потерями, невозможно создать абсолютно безопасную систему защиты от проявления любых угроз. Поэтому вероятность реализации опасных для банка событий будет существовать всегда;
- поскольку проявления разного рода опасностей неизбежны, события злоумышленного характера способны лишь на некоторое время дестабилизировать работу банка, в то время как угрозы внешней среды могут привести к необратимым для него последствиям, вплоть до банкротства [9, с. 94].

Оценка экономической безопасности кредитной организации может проводиться с использованием известных подходов:

- *индикаторный подход*. Оценка экономической безопасности проводится по результатам сравнения фактических показателей учреждения с индикаторами [10, с. 68];

– *ресурсно-функциональный подход*. В соответствии с ним оценка безопасности бизнес-субъекта проводится на основе анализа использования корпоративных ресурсов по специальным критериям. При этом рассматриваются ресурсы капитала, персонала, информации и технологии, техники и оборудования;

– *метод сравнения* расчетной величины реинвестируемой прибыли с объемом средств, нужных для расширенного воспроизводства капитала;

– *подход, отражающий принципы и условия программно-целевого управления и развития*. Оценка экономической безопасности базируется на расчете интегрального показателя. При этом используется несколько уровней интеграции показателей и такие способы их анализа, как кластерный и многомерный анализ².

Резюмируя, отмечаем, что чаще всего как индикаторы негативных тенденций в кредитной организации выступают показатели, используемые для надзора, контроля и стресс-тестирования в банковской системе. Банки могут воспользоваться моделями консалтинговых компаний, материнских банков, профессиональных сообществ [11, с. 118]. Наивысшая степень безопасности достигается при условии, что весь комплекс частных показателей находится в пределах допустимых границ, а пороговые значения одного показателя достигаются не в ущерб другим.

В контексте данного исследования актуальность индикаторного подхода опосредована также тем, что показатели безопасности базируются на системе управления рисками, включая определение ее различных элементов, принципов взаимодействия и распределения полномочий между органами управления и структурными подразделениями.

Одним из важнейших объектов управления в банке выступает кредитный риск, к основным индикаторам которого следует отнести:

- объем размещения в среднесрочном и абсолютном выражении;
- удельный вес ссудной задолженности корпоративных клиентов и физических лиц, просроченной задолженности в общем кредитном портфеле;

² Забродский В., Капустин Н. Теоретические основы оценки экономической безопасности отрасли и фирмы // Бизнес-информ. 1999. № 15. С. 35–37.

- среднюю ставку размещения.

При использовании индикаторного подхода, как отмечалось ранее, проводится сравнение полученных фактических данных с плановыми целевыми показателями в рамках специальной формы отчета. В свою очередь, отчет об уровне кредитных рисков уполномоченные сотрудники департамента кредитования обычно представляют ежеквартально подразделению, управляющему рисками.

На примере одного из региональных банков Волгоградской области – ПАО КБ «РусЮгбанк» – конкретизируем методы регулирования кредитного риска.

Лимитирование. В качестве органов, лимитирующих кредитные операции, выступают совет директоров и кредитный комитет. Последний несет ответственность за утверждение следующих лимитов:

- максимальной суммы кредитов одному или группе взаимосвязанных заемщиков;
- максимального размера риска по отраслям;
- лимитов на отдельные виды и формы кредитования, кредитные продукты;
- лимитов на минимальную и максимальную величины кредита.

Ограничение полномочий в подразделениях кредитования. В данном случае политика банка ориентирована на уменьшение кредитного риска, связанного с принятием ошибочного решения или злоупотреблением должностными полномочиями кредитным менеджером, руководителем кредитного отдела, и призвана обеспечить эффективность управления кредитным риском.

Контроль за реализацией данного метода регулирования кредитного риска возложен на службу внутреннего аудита и кредитное управление банка.

Ограничения по географическому пространству. Приоритеты отраслей и географии операций заложены в Стратегии развития ПАО КБ «РусЮгбанк», утвержденной советом директоров, а также в Кредитной политике ПАО КБ «РусЮгбанк». В табл. 1 и 2 отражено распределение в учреждении кредитного риска по географическому признаку и видам деятельности заемщиков.

Резервирование под ожидаемые потери. С целью минимизации кредитного риска по индивидуальной ссуде банком актуализирована традиционная практика обеспечения ссуды залогом ликвидного имущества, находящимся в собственности как заемщика, так и третьего лица. В табл. 3 приведены данные по стоимости обеспечения, принятого в залог ПАО КБ «РусЮгбанк» в 2015 г.

Следует отметить: несмотря на наличие обеспечения, контроль за кредитным риском индивидуального заемщика реализуют кредитный менеджер, руководитель кредитующей структуры, начальник отдела активных операций. Отчет о мероприятиях, а также о планируемой работе с заемщиками, отнесенными к группам высокой и повышенной степени риска, подлежат рассмотрению кредитным комитетом банка по поручению департамента кредитования.

В деятельности любой кредитной организации всегда присутствует вероятность неисполнения своих обязательств перед контрагентами в полном объеме и в установленный срок в связи с несовпадением сумм поступлений и выплат денежных средств по срокам и в разрезе валют [12, с. 71]. Речь идет о риске ликвидности, управление которым обеспечивается исполнением таких процедур:

– выявление риска методами:

- прогнозирования и анализа состояния объектов риска ликвидности с учетом поведенческих аспектов;
- лимитирования величины высоколиквидных активов;
- прогнозирования способности банка получать ресурсы на рынке межбанковских операций;

– мониторинг риска посредством:

- формирования еженедельного прогноза движения денежных потоков;
- отчета о состоянии ликвидной позиции по временным периодам;
- систематизации данных о соблюдении лимитов;
- сбора ежедневной информации о соблюдении требований в части нормативов;
- накопления ежемесячной информации о величине показателей ликвидности,

определенных в указаниях Банка России № 2005-У³, а также ежеквартальных сведений о величине показателей ликвидности, зафиксированных в указаниях Банка России № 1379-У⁴;

– стресс-тестирование управления ликвидностью.

Управление рыночным риском обеспечивается следующими процедурами:

– выявлением риска посредством:

- анализа конъюнктуры рынка финансовых инструментов и изучения состояния объектов рыночного риска;
- лимитирования допустимых потерь от изменений стоимости финансового портфеля банка;
- обращения к «тревожным показателям», сигнализирующим о приближении лимита к опасному уровню;

– оценкой риска посредством ряда расчетных процедур:

- определения совокупной величины рыночного риска в соответствии со стандартным подходом Банка России;
- выявления размера капитала, необходимого для покрытия рыночного риска, в соответствии с внутренним подходом и учетом рекомендаций Дополнения к Базельскому соглашению по капиталу;

– мониторингом риска посредством:

- ежедневного составления отчетных данных, включающих сведения о совокупной величине рыночного риска;
- расчета капитала для покрытия рыночного риска;
- контроля за «тревожными показателями»;

– стресс-тестированием, в сценарий которого включаются удвоенные максимальные падения котировок инструментов за день, отмеченные в течение календарного года.

³ Об оценке экономического положения банков: указание Банка России от 30.04.2008 № 2005-У (ред. от 09.03.2016).

⁴ Об оценке финансовой устойчивости банка в целях признания ее достаточной для участия в системе страхования вкладов: указание Банка России от 16.01.2004 № 1379-У (ред. от 25.10.2013).

Наряду с названными видами риска в работе кредитной организации и воздействующими на уровень ее экономической безопасности, важно представить также:

– *операционный риск*, порождающий убытки по причине несоответствия внутренних порядков и процедур проведения операций масштабам работы банка, установлениям законодательства либо нарушений этих требований персоналом [13, с. 41];

– *правовой риск*, который, являясь разновидностью операционного, имеет следствием прямые потери банка в виде штрафов, пеней, выплат по решениям судов и компенсаций за причиненный ущерб контрагентам и третьим лицам;

– *риск легализации доходов, полученных преступным путем*, который выступает формой проявления правового риска и представлен двумя разновидностями: риском совершения клиентом операций и угрозой вовлеченности банка и его персонала в легализацию доходов, полученных преступным путем, а также в финансирование терроризма;

– *валютный риск* – вероятность прямых или косвенных потерь, возникающих вследствие изменения курсов валют, по которым банк имеет открытую валютную позицию;

– *процентный риск*, связанный с сокращением чистого процентного дохода или чистой приведенной стоимости банка вследствие неблагоприятного изменения рыночной доходности финансовых инструментов.

Акцентируя внимание на операционном риске, отмечаем его масштабность и вариативность. Доказательством выступают его многочисленные разновидности, которые банки вынуждены принимать во внимание:

– *риск управляемости*, который минимизируется посредством рационализации организационных форм внутренних подразделений банка, регламентацией лимитов разрешенных операций и проведением мониторинга их исполнения;

– *репутационный риск* – вероятность убытков по причине сокращения числа клиентов, уменьшения объемов сотрудничества, ухудшения его условий из-за формирования негативной деловой репутации;

– *риск информационной безопасности*, который порождает потери вследствие незащищенности сведений и IT-инфраструктуры от случайных и преднамеренных событий;

– *риск ДБО* – вероятность потерь вследствие любых причин, приводящих к нештатному функционированию информационных систем банка, используемых для дистанционного банковского обслуживания;

– *комплаенс-риск*.

Опираясь на содержание рекомендаций Базельского комитета по банковскому надзору, заложенных в действующее нормативно-правовое поле российского банковского сообщества⁵, связываем комплаенс-риск с возникновением убытков из-за несоблюдения законодательства внутренних документов кредитной организации, стандартов саморегулируемых организаций, а также в результате применения санкций со стороны надзорных органов.

Факторы возникновения этого вида риска совпадают с первопричинами правового риска, дополненными возможным нарушением документированных этических норм ведения банковской деятельности.

С позиции экономической безопасности эффективный комплаенс-контроль в банке способствует:

- укреплению лояльности клиентов;
- росту доверия к банку и заинтересованности акционеров, инвесторов;
- повышению доверия сотрудников и социума благодаря соблюдению их прав, справедливым мотивационным программам, мероприятиям в сфере социальной ответственности.

Анализ практических подходов к обеспечению экономической безопасности кредитной организации показывает, что большинство российских банков очень тщательно прорабатывает сценарии обозначенных рисков и реализует масштабные программы по управлению ими.

Особо следует остановиться на управлении рисками ДБО.

⁵ Об организации внутреннего контроля в кредитных организациях и банковских группах: положение Банка России от 16.12.2003 № 242-П.

Дистанционное банковское обслуживание в современных условиях формирует банку устойчивые конкурентные преимущества в длительной перспективе. Однако эффективность и результативность работы банка определяется возникновением рисков, синергетический эффект которых может серьезно повлиять на репутацию и платежеспособность учреждения.

Дело в том, что любая система ДБО характеризуется наличием не контролируемых банком пользователей и технологической среды. В платежном процессе помимо информационно-технических ресурсов банка задействованы резервы клиента, подверженность которых угрозам различного вида банк не в состоянии полностью контролировать.

Типичный набор существующих способов получения несанкционированного доступа к информации пользователей систем дистанционного банковского обслуживания представлен следующими позициями:

- внедрение вредоносного кода;
- атаки на систему авторизации;
- перехват управления компьютером клиента, искажение или подмена содержания платежных поручений, фишинг⁶;
- сетевые атаки;
- рассылки электронных сообщений, предлагающих ввести информацию в поля экранных форм либо содержащих вредоносное программное обеспечение;
- преступный сговор с инсайдерами либо недобросовестными сотрудниками⁷.

В любом из этих случаев результат один – несанкционированный платеж создан, подписан и направлен в банк под видом обычного платежа. При этом под несанкционированной операцией, совершенной с использованием систем ДБО, понимается событие, связанное с попыткой списания денежных средств со счета клиента за одну или несколько транзакций.

⁶ Фишинг (англ. phishing, от fishing – рыбная ловля, выуживание) – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям.

⁷ Сызганов В.С., Федоров С.С. Дистанционное банковское обслуживание: развитие, проблемы и риски для кредитных организаций // Современные проблемы экономического и социального развития. 2013. № 9. С. 125–126.

В 2015 г. в Банк России было сообщено о 32,5 тыс. попыток незаконных операций через названные системы на общую сумму 5,13 млрд руб. (против 4,89 тыс. попыток на сумму 1,64 млрд руб. в 2014 г.). Динамика несанкционированных операций с использованием российских систем ДБО отражена на рис. 3.

В общем количестве и объеме названных операций на долю транзакций со счетов хозяйствующих субъектов – юридических лиц приходится менее 5% количества и 74% объема. Самое большое количество несанкционированных действий в системах ДБО со счетов физических лиц отмечается в сегменте от 10 до 50 тыс. руб.

В качестве факторов роста указанного количества в 2015 г. по сравнению с 2014 г. отмечено увеличение числа клиентов, использующих дистанционное банковское обслуживание, применение кредитными организациями различных лимитов и дополнительного подтверждения операций на крупные суммы.

Больше половины несанкционированных операций со счетов юридических лиц (57%) было остановлено в полном объеме до наступления окончательности перевода денежных средств. Напротив, 91% противоправных операций со счетов граждан выявляются клиентами самостоятельно при поступлении информации в банк после списания денежных средств со счетов.

В 2014 г. 23 кредитные организации сообщили о попытках списания денежных средств с корреспондентских счетов, открытых в расчетных центрах платежных систем. Были предприняты попытки списания в общей сложности 213,4 млн руб. Такие атаки носят целевой характер, учитывают специфику процессов отправки и обработки сообщений в платежной системе, а вредоносный код в ряде случаев не выявляется даже средствами антивирусной защиты банка.

Для реагирования на компьютерные инциденты такого рода (CERT) в мировой практике функционируют национальные и частные центры противодействия. В России работают несколько CERT:

- RU-CERT (создан Институтом развития общественных сетей);
- Gov-cert.ru (создан Федеральной службой безопасности);

- частный CERT-GIB (принадлежит Group IB).

Последняя структура имеет опыт сотрудничества в области предотвращения киберпреступлений, реагирования, расследования и защиты с рядом банковских (порядка 20 крупных банков), торговых, телекоммуникационных и медиаорганизаций.

Кроме того, для противодействия кибератакам при Банке России создано новое структурное подразделение Главного управления безопасности и защиты информации – Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере, FinCERT. Основной целью структуры признается формирование единого центра компетенции в рамках информационного взаимодействия Банка России, кредитных и некредитных финансовых организаций, компаний-интеграторов, разработчиков антивирусного программного обеспечения, провайдеров и операторов связи, а также для правоохранительных и иных государственных органов, курирующих информационную безопасность отрасли⁸.

Со стороны государственных структур для обеспечения безопасности поднадзорного банковского сообщества прорабатываются вопросы создания системы сертификации выполнения требований информационной безопасности (создание закона о техническом регулировании), аутсорсинга информационной безопасности для малых и средних банков, расширения идентификации и аутентификации клиента в электронном пространстве с использованием технологий телекомоператоров.

На уровне банка в качестве варианта минимизации рисков несанкционированных платежей выступает мониторинг транзакций, антифрод. Имеется в виду использование максимально доступного количества параметров платежа – как финансовых, так и технических – с регулярным пересмотром и корректировкой действующей модели обнаружения.

Самый простой сценарий: необходимо проанализировать поток клиентских платежей за некоторый период. Если клиент совершает два или более платежа по адресу одного и того же контрагента, нет оснований полагать, что очередной платеж данному контрагенту будет мошенническим. Если же платеж совершается по адресу нового получателя, необходимо получить от клиента дополнительное подтверждение того, что платеж не является мошенническим.

⁸ Шумилина О.В., Езангина И.А. Финансовая безопасность банка: риски ДБО // Научный альманах. 2016. № 2-1. С. 392–396.

Ситуация может быть осложнена, когда платеж проводится на карту физического лица, поскольку в качестве счета получателя может быть указан консолидированный номер счета для расчетов по пластиковым картам. В этом случае номер счета или номер карты получателя указывается в назначении платежа⁹.

Помимо этого, инструментами для незаконного вывода средств могут являться агрегаторы платежей, такие как федеральная система «Город», позволяющие переводить средства клиентов во внешние системы, со счетов которых впоследствии можно вывести средства на карту. Речь идет о системах Qiwi, Yandex.Деньги и т.п.

Платежный документ для банка выглядит как внутренний, счетом получателя является счет 30220 – незавершенные расчеты; в назначении платежа указывается код услуги и номер счета пользователя.

Поскольку поток обрабатываемых платежей может быть большим, при обработке каждого платежа поиск других платежей клиента за заданный промежуток времени может негативно влиять на время обработки. Имеет смысл составить список благонадежных получателей и периодически обновлять его. В этом случае при обработке платежа достаточно проверить присутствие получателя в списке.

С учетом сказанного наиболее целесообразным является для каждого благонадежного получателя хранить банковский идентификационный код банка получателя, счет получателя или номер счета (карты) из назначения платежа.

Для подтверждения платежей, получатели которых не попали в сформированный список, можно использовать звонок менеджера клиенту. Запрос на подтверждение платежа может быть автоматизированным – в этом случае между системой ДБО, автоматизированной банковской системой (АБС) и клиентом состоится обмен сообщениями, отраженный на рис. 4.

⁹ Коняевский В.А. Минимизация рисков участников дистанционного банковского обслуживания // Вопросы защиты информации. 2014. № 4. С. 3–4.

Поскольку ничтожно мала вероятность того, что благонадежный контрагент одного из клиентов может одновременно являться злоумышленником относительно другого клиента, можно вести список благонадежных контрагентов по всему банку, а не для каждого клиента отдельно. В таком случае количество необходимых подтверждений резко сократится [14, с. 59].

Таким образом, безопасность функционирования коммерческих банков должна быть управляемой, а следовательно, надежно обеспеченной¹⁰.

Основу экономической безопасности современного коммерческого банка составляет его финансовая устойчивость, являющаяся следствием действия системы институционально-управленческих, организационно-технических и информационных мер, направленных на обеспечение воспроизводства устойчивого режима работы банка, защиту его прав и интересов, рост уставного капитала, повышение ликвидности активов, сохранность финансовых и материальных ценностей, а также на обеспечение возвратности кредитов.

¹⁰ *Сторожук И.Н.* Механизм обеспечения экономической безопасности коммерческих банков // *Экономический вестник Ростовского государственного университета.* 2009. Т. 7. № 3. С. 142–148.

Таблица 1

Распределение кредитного риска ПАО КБ «РусЮгбанк» по регионам РФ в 2015 г.

Table 1

Distribution of credit risk of PAO KB RusYugbank in regions of Russia in 2015

Регион	Задолженность по ссудам, тыс. руб.	Удельный вес в общем объеме, %
Волгоградская область	4 472 766	81
Краснодарский край	494 171	9
Астраханская область	349 000	6,3
Москва	82 684	1,5
Калининградская область	69 000	1,3
Воронежская область	39 933	0,7
Московская область	10 040	0,2
Саратовская область	1 687	0
Республика Адыгея	167	0
Республика Калмыкия	91	0
Итого...	5 519 539	100

Источник: составлено авторами по материалам Годового отчета ПАО КБ «РусЮгбанк» за 2015 г.

URL: http://www.rsbank.ru/for_investors/god_reporting

Source: Authoring, based on materials of the Annual Report of PAO KB RusYugbank for 2015.

Available at: http://www.rsbank.ru/for_investors/god_reporting

Таблица 2

Распределение кредитного риска ПАО КБ «РусЮгбанк» по видам экономической деятельности в 2015 г.

Table 2

Distribution of credit risk of PAO KB RusYugbank by economic activity of borrowers in 2015

Вид деятельности	На конец отчетного периода, тыс. руб.	Удельный вес в общем объеме, %
Торговля	2 728 849	49,4
Промышленное производство	817 947	14,8
Предоставление услуг, операции с недвижимым имуществом, аренда	506 515	9,2
Сельское хозяйство	477 004	8,6
Строительство	396 986	7,2
Физические лица	273 706	5
Финансовая деятельность	89 336	1,6
Транспорт и связь	74 876	1,4
Прочие виды деятельности	154 320	2,8
Итого...	5 519 539	100

Источник: составлено авторами по материалам Годового отчета ПАО КБ «РусЮгбанк» за 2015 г.

URL: http://www.rsbank.ru/for_investors/god_reporting

Source: Authoring, based on materials of the Annual Report of PAO KB RusYugbank for 2015.

Available at: http://www.rsbank.ru/for_investors/god_reporting

Таблица 3

Стоимость обеспечения, принятого в залог ПАО КБ «РусЮгбанк» в 2015 г.

Table 3

Cost of collateral accepted by PAO KB RusYugbank in 2015

Вид обеспечения	Стоимость залогового обеспечения, тыс. руб.	Удельный вес в общем объеме, %
Поручительство	30 543 068	78,8
Имущество, в том числе:	8 161 969	21,1
– недвижимость	5 541 215	14,3
– товары в обороте	1 099 345	2,8
– спецтехника, транспорт	959 747	2,5
– оборудование	491 662	1,3
– прочее	70 000	0,2
Финансовые инструменты (ценные бумаги)	35 042	0,1
Итого...	38 740 079	100

Источник: составлено авторами по материалам Годового отчета ПАО КБ «РусЮгбанк» за 2015 г.

URL: http://www.rsbank.ru/for_investors/god_reporting

Source: Authoring, based on materials of the Annual Report of PAO KB RusYugbank for 2015.

Available at: http://www.rsbank.ru/for_investors/god_reporting

Рисунок 1

Внешние факторы безопасности коммерческого банка

Figure 1

External security factors of commercial banks



Источник: авторская разработка

Source: Authoring

Рисунок 2

Внутренние факторы безопасности коммерческого банка

Figure 2

Internal security factors of commercial banks



Источник: авторская разработка

Source: Authoring

Рисунок 3

Динамика количества и объема несанкционированных операций, совершенных с использованием систем ДБО в России в 2014–2015 гг.

Figure 3

Change in number and volume of unauthorized transactions using remote banking service systems in Russia in 2014–2015



Источник: составлено авторами по материалам обзора Банка России о несанкционированных переводах денежных средств 2015 г. URL: http://www.cbr.ru/PSystem/P-sys/survey_2015.pdf

Source: Authoring, based on materials of the Bank of Russia's review on unauthorized transfer of funds in 2015. Available at: http://www.cbr.ru/PSystem/P-sys/survey_2015.pdf

Рисунок 4

Автоматизированный алгоритм запроса платежа в системе ДБО

Figure 4

Automated payment request algorithm in the system of RBS



Источник: авторская разработка

Source: Authoring

Список литературы

1. *Подмолодина И.М., Воронин В.П., Коновалова Е.М.* Подходы к оценке экономической безопасности предприятий // Вестник Воронежского государственного университета инженерных технологий. 2012. № 4. С. 156–161.
2. *Домашова Д.В., Самошина Е.О.* Формирование оптимальной стратегии системы обеспечения экономической безопасности коммерческого банка // Безопасность информационных технологий. 2011. № 4. С. 93–96.
3. *Хачатурян Г.Ю.* Институциональные основы экономической безопасности банковской деятельности в современной экономике // Вестник университета (государственный университет управления). 2010. № 21. С. 15–22.
4. *Ведерникова Т.В.* Управление экономической и финансовой безопасностью банков // Инновационное развитие экономики. 2014. № 2. С. 97–101.
5. *Арефьева О.В., Кузнецов Т.Б.* Планирование экономической безопасности предприятий: монография. Москва: Изд-во Европ. ун-та, 2004. 170 с.
6. *Погребенко Ю.Н.* Основные направления и пути обеспечения экономической безопасности деятельности коммерческих банков // Бизнес в законе. Экономико-юридический журнал. 2012. № 2. С. 365–367.
7. *Красноперова Т.Я.* Реальный интерес. Воздействие экономических интересов на состояние экономической безопасности банка // Российское предпринимательство. 2008. № 8-1. С. 29–33.
8. *Миляев П.В.* Экономическая безопасность коммерческого банка в системе национальной безопасности государства // Аудит и финансовый анализ. 2010. № 2. С. 442–445.
9. *Овчинников В.Н., Сторожук И.Н.* Управление экономической безопасностью коммерческого банка в условиях финансового кризиса: монография. Р/Д: Южный Федеральный университет, 2013. 192 с.
10. *Дресвянникова Г.С.* Особенности использования различных показателей для оценки уровня экономической безопасности предприятий и организаций / Череповецкие научные чтения – 2012: м-лы науч.-практ. конф. Череповец: Череповецкий гос. ун-т, 2013. С. 67–70.
11. *Андреева Е.А.* Индикаторы экономической безопасности многофилиального банка с иностранным участием // Вестник Института экономики Российской академии наук. 2014. № 4. С. 116–125.
12. *Фрумина С.В.* Риски коммерческого банка, влияющие на экономическую безопасность: современная практика минимизации // Проблемы анализа риска. 2010. Т. 7. № 2. С. 66–77.
13. *Смагина М.Н., Сорина Е.И., Золотарева Г.М.* Внутренний аудит и менеджмент операционных рисков системы дистанционного банковского обслуживания // Вестник Тамбовского университета. Серия: Гуманитарные науки. 2015. № 8. С. 38–44.
14. *Езангина И.А.* Потенциал сетевой модели организации и управления межфирменным взаимодействием / Актуальные вопросы развития социально-экономических систем в современном обществе: м-лы науч.-практ. конф. Саратов: Центр профессионального менеджмента «Академия бизнеса», 2014. С. 55–62.

**ECONOMIC SECURITY OF THE CREDIT INSTITUTION:
FACTORS, THREATS, ENHANCEMENT MEASURES**

Sergei P. SAZONOV^a, Irina A. EZANGINA^{b,*}, Roman S. EVSEEV^c

^a Volgograd State Technical University, Volgograd, Russian Federation
sazonovsp@mail.ru

^b Volgograd State Technical University, Volgograd, Russian Federation
ezanginaia@rambler.ru

^c Volgograd State Technical University, Volgograd, Russian Federation
roman.evseev@mail.ru

* Corresponding author

Article history:

Received 27 July 2016

Received in revised form

3 August 2016

Accepted 11 August 2016

JEL classification: G20, G21,
O16

Keywords: economic security,
indicator approach, banking risk,
remote banking, unauthorized
operation

Abstract

Subject The article deals with the issues of ensuring the economic security of credit organizations.

Objectives The paper aims to bring up to date the concept of economic security, approaches to its definition, risks, threats, management practices in relation to the modern commercial bank.

Methods To consider the problem, we used the systems and functional approach within which we applied scientific methods of abstraction, analysis, synthesis, induction, and deduction.

Results We prove that the security level of a modern Bank along with traditional types of risk, as permanent control objects, gets affected by new types of threats, especially the remote banking risk. We identified and clarified the specificity of the concept of banking economic security.

Conclusions and Relevance The main method of evaluating the security of a credit organization is the indicator approach used in the management of traditional risks. The various intruders with criminal intent of unauthorized access, implemented via remote banking services, make an integrated approach to managing the Bank's customer base absolutely essential, to ensure the confidentiality, integrity, authenticity of bank information, and the economic security. The results can be taken into account in the financial policy of the credit organization, especially in remote banking risk management solutions.

© Publishing house FINANCE and CREDIT, 2016

References

1. Podmolodina I.M., Voronin V.P., Konovalova E.M. [Approaches to the evaluation of economic security companies]. *Vestnik Voronezhskogo gosudarstvennogo universiteta inzhenernykh tekhnologii = Bulletin of Voronezh State University of Engineering Technology*, 2012, no. 4, pp. 156–161. (In Russ.)
2. Domashova D.V., Samoshina E.O. [Formation of an optimal strategy for the economic security of the commercial bank system]. *Bezopasnost' informatsionnykh tekhnologii = Safety of Information Technology*, 2011, no. 4, pp. 93–96. (In Russ.)
3. Khachatryan G.Yu. [The institutional foundations of economic security of banking activities in the modern economy]. *Vestnik universiteta (Gosudarstvennyy universitet upravleniya) = University Vestnik (State University of Management)*, 2010, no. 21, pp. 15–22. (In Russ.)
4. Vedernikova T.V. [Management of economic and financial security of banks]. *Innovatsionnoe razvitie ekonomiki = Innovative Development of Economy*, 2014, no. 2, pp. 97–101. (In Russ.)
5. Arefeva O.V., Kuzenko T.B. *Planirovanie ekonomicheskoi bezopasnosti predpriyatii: monografiya* [Planning for the economic security of an enterprise: a monograph]. Moscow, European University Publ., 2004, 170 p.
6. Pogrebenko Yu.N. [The main directions and ways to ensure the economic security of the commercial banks' activities]. *Biznes v zakone. Ekonomiko-yuridicheskij zhurnal = Business in Law. Economics and Law Journal*, 2012, no. 2, pp. 365–367. (In Russ.)
7. Krasnoperova T.Ya. [Real interest. The impact of the economic interests of the State on the economic security of the bank]. *Rossiiskoe predprinimatel'stvo = Russian Journal of Entrepreneurship*, 2008, no. 8-1, pp. 29–33. (In Russ.)

8. Milyaev P.V. [The economic security of a commercial bank in the national security system]. *Audit i finansovyi analiz = Audit and Financial Analysis*, 2010, no. 2, pp. 442–445. (In Russ.)
9. Ovchinnikov V.N., Storozhuk I.N. *Upravlenie ekonomicheskoi bezopasnost'yu kommercheskogo banka v usloviyakh finansovogo krizisa: monografiya* [Economic security management of a commercial bank in the financial crisis: a monograph]. Rostov-on-Don, Southern Federal University Publ., 2013, 192 p.
10. Dresvyannikova G.S. [Features of the use of different indicators to assess the economic security of enterprises and organizations]. *Cherepovetskie nauchnye chteniya – 2012* [Proc. Sci. Conf. Cherepovets Scientific Readings – 2012]. Cherepovets, Cherepovets State University Publ., 2013, pp. 67–70.
11. Andreeva E.A. [Indicators of economic security of the high-street bank with foreign ownership]. *Vestnik Instituta ekonomiki Rossiiskoi akademii nauk = Bulletin of Institute of Economics of Russian Academy of Sciences*, 2014, no. 4, pp. 116–125. (In Russ.)
12. Frumina S.V. [Commercial bank risk to economic security: the modern practice of minimizing]. *Problemy analiza riska = Risk Analysis Problems*, 2010, no. 2, pp. 66–77. (In Russ.)
13. Smagina M.N., Sorina E.I., Zolotareva G.M. [Internal audit and management of operational risk of the e-banking system]. *Vestnik Tambovskogo universiteta. Seriya: Gumanitarnye nauki = Vestnik of Tambov University. Series: Humanities*, 2015, no. 8, pp. 38–44. (In Russ.)
14. Ezangina I.A. [The potential of the network model of organization and management of inter-firm interaction]. *Aktual'nye voprosy razvitiya sotsial'no-ekonomicheskikh sistem v sovremennom obshchestve* [Proc. Sci. Conf. Topical Issues of Socio-Economic Systems in Modern Society]. Saratov, Tsentr professional'nogo menedzhmenta Akademiya Biznesa Publ., 2014, pp. 55–62.