DOI: http://dx.doi.org/10.21686/2413-2829-2025-1-73-88

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ БАНКОВСКОЙ ДЕЯТЕЛЬНОСТИ С УЧЕТОМ НОВЫХ ФАКТОРОВ ДИНАМИЧНО МЕНЯЮЩЕЙСЯ СРЕДЫ

И. В. Ващекина, А. Н. Ващекин
Российский государственный университет правосудия,
Москва, Россия

Цель исследования – классификация источников опасности и угроз для банковской деятельности, выделение основных функциональных целей, достижение которых обеспечивает безопасность банковской деятельности в динамично меняющихся условиях. Авторами применены методы сравнительного анализа, формально-логический, индуктивный, а также математические методы – матричного, графического и нечеткого моделирования. В результате определены цели и предложены меры, способствующие формированию комплексной безопасности банковской деятельности. Однако указанные цели не могут быть достигнуты одномоментно и окончательно, поэтому обеспечение безопасности представляет собой непрерывную смену мероприятий циклического характера. Динамично меняющиеся условия внешней среды банка повышают значение оценки его руководством внешних угроз (в том числе внешнеполитических и даже глобальных). Для предупреждения этих угроз действий отдельного банка недостаточно, однако определение уровня их опасности и проработка мер по реагированию лежат на высшем менеджменте организации, что порождает необходимость изменения структуры органов управления, схемы соподчиненности и ответственности подразделений банка в целях повышения вовлеченности руководства в работу органов безопасности. Практическая классификация источников опасности и угроз для банковской деятельности проводится с помощью матрицы угроз, разработка которой позволяет охарактеризовать основные источники угроз и объекты посягательств. Приведен пример такой матрицы и на ее основе предложена математическая модель, сочетающая нечеткие оценки и точные значения, позволяющие получать согласованное решение. Результат моделирования показывает, какие меры по обеспечению банковской безопасности являются в текущий момент наиболее важными и в какой последовательности их необходимо принимать.

Ключевые слова: банк, безопасность функционирования, угрозы и риски, объекты посягательства, матрица угроз, модель, нечеткие множества.

PROVIDING SECURITY OF BANKING IN VIEW OF NEW FACTORS OF FAST CHANGING ENVIRONMENT

Irina V. Vashchekina, Andrei N. Vashchekin
The Russian State University of Justice, Moscow, Russia

The goal of the research is to classify sources of hazard and threats for banking, to identify key functional targets, whose attainment could provide security of banking in fast changing environment. In the research the authors used methods of comparative analysis, formal-logical, inductive ones, as well as mathematic methods – matrix, graphic and fuzzy modeling. As a result goals were defined and steps proposed that could foster shaping of complex security of banking. However, the mentioned goals cannot be reached at once and finally, thus provision of security is a continuous succession of steps of cyclic nature. Dynamically changing conditions of the external environment of the bank raises the importance of estimating external threats by the top management, including foreign-policy and even global ones. To prevent those threats activities of a single bank will not be enough, however, top management of the organization is responsible for finding the level of their hazard and working-out steps of response, which gives rise to the necessity to change the structure of managerial bodies, the scheme of subordination and responsibility of bank divisions in order to raise involvement of management in operation of security bodies. Practical classification of sources of hazard and threats for banking is conducted by matrix of threats, whose

elaboration could help characterize key sources of threats and objects of infringement. An example of such a matrix was given and on its basis a mathematic model was put forward, which combines fuzzy estimations and accurate values that provide coordinated decisions. The result of modeling shows which steps aimed at providing banking security are now the most important and in what order they shall be taken.
Keywords: bank, security of functioning, threats and risks, objects of infringement, threat matrix, model, fuzzy set.

Введение

Задача обеспечения безопасности функционирования кредитного учреждения всегда рассматривалась как важнейшая. Стабильно высокий уровень количества преступлений в финансово-кредитной сфере, а также доля их среди всех преступлений, совершаемых в стране, фиксируются как сотрудниками правоохранительных органов, так и банковским сообществом[1]. Особенно активизировался рост мошеннических операций с приходом пандемии (только за 2020 г. более чем на 75%[2]). За 2021 г. количество киберпреступлений в России выросло в 1,8 раза, причем на 91% выросло число преступлений с использованием Интернета и на 88% – с применением мобильных телефонов. В 2022 г. их количество несколько снизилось (чему, по мнению Министерства внутренних дел Российской Федерации, способствовало постепенное повышение осведомленности населения о мошеннических приемах телефонных и интернет-мошенников). Однако с учетом предыдущего роста преступность продолжает наносить огромный ущерб, причем Генпрокуратура Российской Федерации признает, что в состоянии расследовать только 25% из них[3]. Обнародованная в конце января 2023 г. Министерством внутренних дел Российской Федерации статистика по преступности в стране свидетельствует о том, что показатели киберпреступности в целом остаются стабильными; с использованием высоких технологий совершается каждое четвертое преступление. А с учетом современной внешнеполитической обстановки и активизации враждебных экономических действий антироссийской коалиции, контролирующей мощные рычаги финансового воздействия и не стесняющейся в использовании всевозможных средств, подрывающих стабильную работу банковской системы и ее отдельных элементов, задача обеспечения безопасности становится первостепенной. Для ее решения банк должен опираться на все доступное ему многообразие располагаемых корпоративных ресурсов, выступающих действующими факторами и способствующих достижению главных целей банковского бизнеса.

Литературный обзор

Проблемы укрепления безопасности банковской деятельности активно обсуждаются в современной научной литературе. При этом отмечается важность успешного решения этих проблем в рамках отдельных кредитных организаций для обеспечения безопасности всей банковской системы на государственном уровне [8; 21], а также ведущая роль, которую она играет в поддержании стабильного функционирования экономики [9].

Безопасная банковская деятельность рассматривается в экономическом [10; 16], финансовом [17] и правовом [13; 18] аспектах. Большое внимание уделяется вопросам внедрения новых технологий обеспечения безопасности [11; 19], новых приемов и методов управления, повышающих безопасность банковской работы [2; 7]. С учетом развития информационного общества и цифровизации всех типов экономических взаимодействий активно обсуждаются как негативные (играющие на руку злоумышленникам) [1; 12], так и позитивные (повышающие возможности службы

[1] URL: https://www.ng.ru/economics/2021-08-03/1_8215_economics2.html (дата обращения: 18.03.2024).
[2] URL: https://www.rbc.ru/society/31/08/2020/5f48ea169a79477e21e25d9d (дата обращения: 18.03.2024).
[3] URL: https://www.tadviser.ru/index.php/Статья:Число_киберпреступлений_в_России# (дата обращения: 18.03.2024).

безопасности банка) [6] стороны этого явления.

Функциональные цели экономической безопасности

Несомненно, главными результатами мероприятий по обеспечению экономической безопасности в каждом банке при любых условиях должны оставаться поддержание стабильной и эффективной его работы в текущий момент, а также сохранение необходимого потенциала развития в целях перспективного роста в будущем даже на фоне частичного оттока клиентов и денежных средств – проблемы, характерной для всех российских банков в настоящий момент. Наиболее эффективное распределение корпоративных ресурсов, гарантирующее достижение целей банковского бизнеса, может быть только при условии предотвращения всех внешних и внутренних угроз его экономической безопасности, предупреждения их возникновения в будущем и предотвращения возможных негативных последствий в случае их осуществления. Функциональные цели экономической безопасности должны быть связаны со следующими направлениями работы банка:

- сотрудники;
- система менеджмента;
- капитал и иное имущество;
- коммерческие интересы;
- финансовая независимость;
- корпоративные НИОКР;
- технологическое совершенство;
- правовое обеспечение деятельности;
- информационная среда (цифровое поле и иные виды коммуникаций).

Каждая цель экономической безопасности банка должна содержать в себе структурированный набор подцелей, нередко уникальный, поскольку он определяется как характером самой цели, так и специализацией конкретного банка.

Необходимо также учитывать, что цели не могут быть достигнуты одномоментно и окончательно, поэтому обеспечение их безопасности в реальных условиях динамично меняющейся среды представляет собой непрерывную смену мероприятий, многие из которых носят циклический характер. То есть комплекс мероприятий должен быть так систематизирован и скоординирован, чтобы организация их выполнения, контроля и прогнозирования гарантировала постоянный уровень безопасности банка.

Схематически работа по обеспечению экономической безопасности банка показана на рис. 1, из которого видно, что цели банковского бизнеса формируют его философию (легальную или нелегальную, декларируемую или фактически проводимую), реализация которой определяется потенциалом корпоративных ресурсов, состоящим из следующих элементов:

а) *капитал* – комбинация акционерного капитала банка и заемных ресурсов, которая обеспечивает устойчивое финансовое положение банка, создавая возможности для приобретения всех остальных корпоративных ресурсов, а также их поддержки в работоспособном состоянии;

б) *персонал* – сотрудники и менеджеры, обладающие необходимой квалификацией, обеспечивающие слаженное взаимодействие всех компонентов банковского бизнеса и совместно стремящиеся к достижению его целей;

в) *право* – юридическая защита ценных для бизнеса интеллектуальных объектов, как материальных, так и нематериальных, которая образует важный ресурс, обеспечивающий их использование (нередко исключительное) в интересах бизнеса;

г) *информация и технологии* – наиболее ценный и часто весьма дорогостоящий ресурс, который в цифровую эпоху становится решающим фактором развития банка (сведения о динамике политической и экономической обстановки, передовые разработки в области технологий, имеющиеся в распоряжении банка ноу-хау, уникальные методики организации и управления – все это позволяет своевременно реагировать на любые изменения внешней среды бизнеса, производить дол-

госрочное планирование и обеспечивать эффективную его работу);

д) *техника и оборудование* – качество этого ресурса, его обслуживание и эффективность его использования в значительной степени определяются финансовыми, информационно-технологическими и кадровыми возможностями банка.

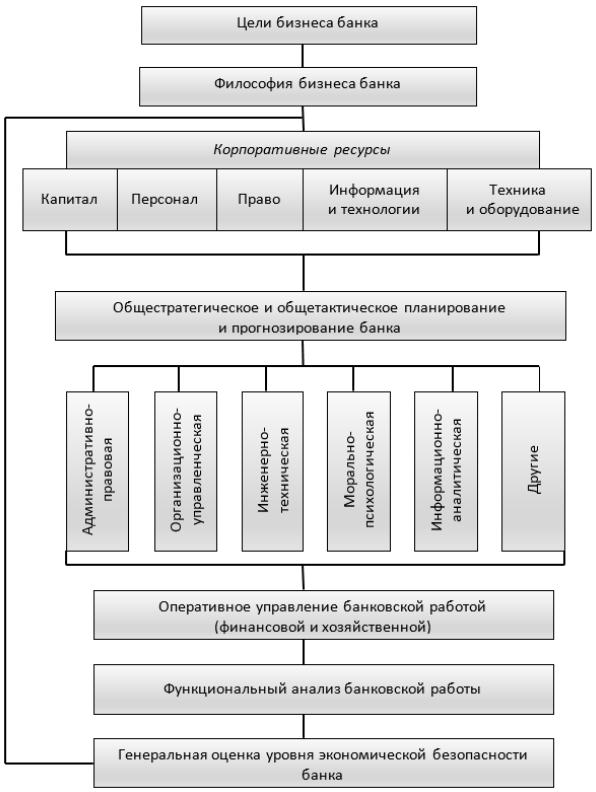

Рис. 1. Процесс обеспечения экономической безопасности банка

О комплексной безопасности банковской деятельности

Из проведенного анализа отдельных компонентов, функций и направлений банковской безопасности следует, что особое значение в условиях динамично меняющейся среды приобретает формирование комплексной безопасности банковской деятельности. Комплексность предполагает наличие системы предупредительных мероприятий, которые на постоянной основе одновременно и непрерывно осуществляются специальными силами безопасности и персоналом банка, обеспечивают условия для наиболее эффективного ведения банковской деятельности, способствуют повышению уровня защиты безопасности банка от всех видов угроз и снижению всех видов рисков. В рамках этой концепции неизбежно создание специальных сил безопасности, которые представляют собой негосударственные структуры, выполняющие охранные и детективные задачи (предупреждение возможных угроз и расследование постфактум), обладающие квалифицированным людским и современным материально-техническим потенциалом. Они должны вести свою работу в рамках действующего законодательства в тесном взаимодействии с государственными правоохранительными органами, а в определенных ситуациях – под их руководством.

Для достижения комплексной безопасности необходимо обеспечить:

– защиту банковского персонала и менеджмента от возможных угроз всеми доступными законными средствами;

– сохранность материальных и финансовых ресурсов;

– закрытость значимых информационных ресурсов на протяжении их жизненного цикла, секретность данных на всех этапах их обработки;

– способность системы к совершенствованию на основе стратегии развития банка с учетом динамично меняющихся условий среды.

Комплексность может быть достигнута:

– установлением диктуемого обстоятельствами режима охраны;

– применением специальных форм делопроизводства, обеспечивающих защиту банковских секретов;

– осмотрительным подбором и расстановкой кадров;

– внедрением передовых технических средств, в первую очередь в области защиты цифровых данных;

– ведением информационно-аналитической деятельности;

– своевременными и результативными действиями по расследованию любых нештатных ситуаций.

Безопасность каждого банка имеет свою специфическую экономико-правовую направленность, состоящую из ряда элементов, таких как:

– порядок создания и ликвидации банка;

– процедура контроля за работой кредитной организации;

– регулирование деятельности кредитной организации с помощью устанавливаемых экономических нормативов;

– составление финансовой отчетности и ее открытость;

– комплекс мер (методика) предотвращения кризисных ситуаций и их профилактика;

– возможности и порядок осуществления защиты операций клиентов, застрахованных лиц и пр.

Особую важность среди мероприятий по предупреждению кризиса банка имеют анализ угроз и рисков банковской деятельности, охрана банковских объектов и предотвращение нанесения ущерба деятельности банка. Внутренние и внешние угрозы деятельности банка представлены на рис. 2.

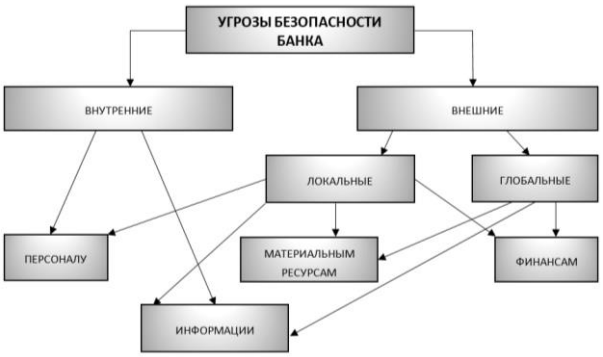

Рис. 2. Угрозы безопасности банка

Среди угроз персоналу, например, можно привести этические и телесные страдания, убийства, похищения сотрудников и их близких; угрозы, запугивания, шантаж и вымогательство. Примером угрозы материальным ресурсам может служить повреждение или уничтожение недвижимого и движимого имущества, коммуникаций и транспортных средств; угрозы финансам – кража, блокировка или временный увод финансовых средств и иных ценностей, а также мошенничество, подделка финансовых документов. Среди информационных угроз можно указать снятие защиты и получение несанкционированного доступа к охраняемым данным, уничтожение этих данных или их модификацию с криминальными целями.

На рис. 2 показана лишь общая схема, фактически же работа банка сопровождается очень большим количеством рисков, связанных с внутренними и внешними факторами, влияющими на работу банка и способными вызвать проблемы с ликвидностью и (или) финансовые убытки. Для снижения этих рисков Банк России издает рекомендации, которые должны быть положены в основу работы коммерческих банков в области внутреннего контроля за рисками. Однако эти рекомендации не могут считаться исчерпывающими – оценка рисков должна оставаться в ряду первостепенных текущих задач в работе любого банка.

Построение матрицы угроз

В целях практической классификации различных источников опасности и угроз для банковской деятельности необходимо разработать матрицу угроз, которая позволяет охарактеризовать основные источники угроз и объекты посягательств. Пример такой матрицы представлен в таблице. Матрица угроз может быть максимально эффективно использована при формировании специальных кризисных планов. При этом могут разрабатываться мероприятия, которые облегчают действия персонала банка под воздействием угроз разного уровня и направленности.

Матрица угроз

Объекты посягательства. Источники угроз	**Материальные ресурсы (O_1)**	**Персонал (O_2)**	**Информация (O_3)**	**Технические и программные средства вычислительной техники (O_4)**	**Средства связи и телекоммуникации (O_5)**	**Иные технические средства (O_6)**	**Здания, помещения, хранилища (O_7)**	**Система управления (O_8)**
Криминальные структуры, потенциальные преступники (U_1)	Хищение, кража, мошенничество, подлог	Оказание давления, физическое уничтожение	Хищение носителей информации, несанкционированное получение информации с применением специальной аппаратуры или во время пребывания в банке, мошенничество, подлог, препятствование использованию, сбор мусора	Физическое разрушение, хищение, подлог	Вывод из строя системы сигнализации, перехват сообщений	Прямое хищение	Физическое проникновение	Воздействие на персонал путем коммерческого подкупа, угроз, шантажа и т. п.
Конкуренты (U_2)	Срыв деловых сделок, скупка акций, мошенничество, подлог	Подкуп персонала	Ознакомление с конфиденциальной информацией во время пребывания в банке, несанкционированное получение информации с применением специальной аппаратуры, мошенничество, подлог, сбор мусора	Нанесение вреда программному обеспечению, пиратство, подлог	Прослушивание, перехват сообщений	Перехват сообщений	Съем информации	Дезинформация
Недобросовестные контрагенты (U_3)	Неуплата, мошенничество, подлог	Подкуп персонала	Использование конфиденциальной информации в собственных интересах, мошенничество, небрежность, подлог, сбор мусора	Поставка нелицензионных программных продуктов, небрежность, пиратство, подлог	Прослушивание, перехват сообщений	Перехват сообщений	Съем информации	Предоставление искаженной информации, нарушение системы управления
Персонал (U_4)	Пособничество в хищении, прямое хищение, мошенничество, подлог, низкая квалификация	Использование служебного положения в личных целях, низкая квалификация	Хищение документов, носителей информации, неосознанное разглашение информации, снятие копий с документов, выброс в мусор черновиков, магнитных и электронных носителей, мошенничество, небрежность, подлог, препятствование использованию, сбор мусора, низкая квалификация	Нарушение работоспособности технических средств по халатности или злому умыслу, небрежность, пиратство, подлог, умышленное повреждение данных или программ, низкая квалификация	Прослушивание, перехват сообщений, низкая квалификация	Вывод из строя по заданиям конкурентов или под давлением, низкая квалификация	Нарушение прав допуска, низкая квалификация	Использование недостатков системы управления, халатное отношение к функциональным обязанностям, самоуправство, низкая квалификация
Техногенные (U_5)	Глобальные техногенные воздействия	Непредвиденные расходы	Нарушение режима работы, временная нетрудоспособность и гибель персонала	Уничтожение	Уничтожение, аппаратные сбои, ошибки программ	Уничтожение, аппаратные сбои, ошибки программ	Уничтожение, аппаратные сбои, ошибки программ	Уничтожение
Стихийные (U_6)	Природные катаклизмы	Непредвиденные расходы, пожары, наводнения	Нарушение режима работы, временная нетрудоспособность и гибель персонала	Полная или частичная потеря информации при пожаре, наводнении	Физическое разрушение	Физическое разрушение	Физическое разрушение	Физическое разрушение

Адекватности в оценке уровня различных угроз финансовой и банковской безопасности можно добиться путем применения математического моделирования [15]. В этой сфере наиболее эффективными, как показывает практика, оказываются модели, построенные на основе комбинации теории нечетких множеств [20] и метода анализа иерархий [14]. Суть методики нечетких множеств – превращение субъективных (нечетких) экспертных оценок в числовые значения и проведение вычислений, приводящих к согласованному решению [5].

На основе нечеткого подхода в контексте данной статьи авторы предлагают построить математическую модель, дающую представление о том, какие меры по обеспечению банковской безопасности являются в текущий момент наиболее важными, и приводящую к определению, в какой последовательности их необходимо принимать.

Математическая модель

Эту задачу в формальной записи можно представить следующим образом.

Пусть $O = \{O_1, O_2, \ldots, O_n\}$ – множество объектов посягательства;

$U = \{U_1, U_2, \ldots, U_m\}$ – множество угроз;

$P = \{P_1, P_2, \ldots, P_p\}$ – множество признаков, характеризующих эти объекты и угрозы.

В вышеприведенном примере матрицы угроз множество объектов образовано восемью элементами ($n = 8$), а множество угроз включает шесть элементов ($m = 6$). Количество признаков зависит от точности модели (чем их больше, тем адекватнее будет результат). Для каждой группы объектов целесообразно подбирать свой уникальный набор признаков. Нетрудно заметить, что не каждый признак характерен для любого объекта.

Пусть α: $O \cdot P \rightarrow [0; 1]$ – функция принадлежности нечеткого бинарного отношения A, которая задается экспертом по безопасности (или группой экспертов). Значения этой функции показывают, в какой степени конкретному объекту O_i присущ признак P_j. Запишем эти значения по каждому O_i в строку, затем расположим эти строки в порядке нумерации O_i друг под другом. Получим матрицу значений A:

$$A = \begin{array}{c} \\ O_1 \\ O_2 \\ \ldots \\ O_n \end{array} \begin{array}{c} \begin{array}{cccc} P_1 & P_2 & \ldots & P_p \end{array} \\ \begin{pmatrix} \alpha_{11} & \alpha_{12} & \ldots & \alpha_{1p} \\ \alpha_{21} & \alpha_{22} & \ldots & \alpha_{2p} \\ \ldots & \ldots & & \ldots \\ \alpha_{n1} & \alpha_{n2} & & \alpha_{np} \end{pmatrix} \end{array}.$$

Аналогично: пусть β: $P \cdot U \rightarrow [0; 1]$ – функция принадлежности нечеткого бинарного отношения A, которая задается экспертом по безопасности (или группой экспертов). Значения этой функции показывают, в какой степени каждый признак объекта P_j создает уязвимость от угрозы U_k. Значения этой функции образуют матрицу B:

$$B = \begin{array}{c} \\ P_1 \\ P_2 \\ \ldots \\ P_p \end{array} \begin{array}{c} \begin{array}{cccc} U_1 & U_2 & \ldots & U_m \end{array} \\ \begin{pmatrix} \beta_{11} & \beta_{12} & \ldots & \beta_{1m} \\ \beta_{21} & \beta_{22} & \ldots & \beta_{2m} \\ \ldots & \ldots & & \ldots \\ \beta_{p1} & \beta_{p2} & & \beta_{pm} \end{pmatrix} \end{array}.$$

Для оценки уровня каждой конкретной угрозы U_i необходимо построить множества M_{Ui}, элементами которых будут такие объекты O_j, которые наиболее уязвимы для угрозы U_i.

Решение этой задачи происходит следующим образом.

Из данных в условии матриц A и B вычисляем матрицу Ω:

$$\Omega = \begin{array}{c} \\ O_1 \\ O_2 \\ \ldots \\ O_m \end{array} \begin{array}{c} \begin{array}{cccc} U_1 & U_2 & \ldots & U_n \end{array} \\ \begin{pmatrix} \omega_{11} & \omega_{12} & \ldots & \omega_{1n} \\ \omega_{21} & \omega_{22} & \ldots & \omega_{2n} \\ \ldots & \ldots & & \ldots \\ \omega_{m1} & \omega_{m2} & & \omega_{mn} \end{pmatrix} \end{array},$$

элементы которой равны

$$\omega = \frac{\sum_P \alpha(O, P) \cdot \beta(P, U)}{\sum_P \alpha(O, P)}.$$

Числитель этой дроби является результатом произведения матриц A и B, а знаменатель представляет собой сумму элементов соответствующей строки матрицы A. К такой нормировке необходимо приводить матрицу Ω для того, чтобы ее элементы оставались в пределах отрезка [0; 1].

Далее формируется матрица попарных минимумов Δ. В ней каждый элемент поочередно сравнивается со всеми элементами, стоящими в той же строке матрицы Ω правее его:

$$\Delta = \begin{pmatrix} \min(\omega_{1,1}, \omega_{1,2}) & \dots & \min(\omega_{1n-1}, \omega_{1,n}) \\ \dots & \dots & \dots \\ \min(\omega_{m,1}, \omega_{m,2}) & \dots & \min(\omega_{m,n-1}, \omega_{m,n}) \end{pmatrix}.$$

Критерий значимости угроз δ ограничивается условием

$$\delta < \min_{i,j} \max_{O} \min(\omega(O, U_i), \omega(O, U_j)).$$

Таким образом, в матрице Δ вычисляется максимум среди элементов каждого столбца (эта процедура дает нам несколько чисел), затем определяется минимум из этих чисел (что оставляет нам одно число), а затем в матрице A находится элемент, чуть меньший этого числа. Он и будет служить критерием отбора δ.

После того, как критерий δ выбран, мы можем для каждой угрозы U_i построить множества M_{Ui}, включающее в себя угрожаемые объекты, и видеть в численном выражении степень опасности для каждого из них:

$$M_{Ui} = \left\{ P \mid \omega(O, U_i) \geq \min_{i,j} \max_{O} \min(\omega(O, U_i), \omega(O, U_j)) \right\}$$

Приведенный формальный математический метод сглаживает субъективные экспертные оценки и позволяет сконцентрировать основные усилия по обеспечению безопасности на наиболее угрожаемых направлениях работы кредитно-финансовой организации.

Численный пример

Рассмотрим более подробно угрозы объектам из объединенных групп O_4 (технические и программные средства вычислительной техники) и O_5 (средства связи и телекоммуникации). Среди этих объектов выделим, перенумеровав, следующие: O_1 – база данных клиентов; O_2 – база данных контрагентов; O_3 – база данных сотрудников; O_4 – средства обеспечения дистанционного банковского обслуживания; O_5 – средства взаимодействия с контрагентами; O_6 – средства внутренней коммуникации банка; O_7 – средства обеспечения информационной безопасности.

В качестве признаков этих объектов возьмем следующие: P_1 – связь с открытыми данными; P_2 – многочисленность пользователей; P_3 – частота инцидентов на объекте; P_4 – физическая доступность объекта; P_5 – незащищенность виртуального доступа к объекту; P_6 – коррупционная (инсайдерская) уязвимость.

Основные угрозы, рассматриваемые в нашем примере, таковы: U_1 – вредители (имеются в виду действующие извне хакеры, стремящиеся нанести ущерб без прямой выгоды для себя); U_2 – вымогатели (лица или организации, способные поставить под угрозу деятельность банка и потребовать денежные средства за снятие этой угрозы); U_3 – похитители (преступники, тайно осуществляющие изъятие средств банка, его клиентов или контрагентов); U_4 – недобросовестные контрагенты (организации, использующие незаконно полученную информацию для получения более выгодной позиции на переговорах); U_5 – персонал (сотрудники, совершающие ошибки вследствие непрофессионализма, рассеянности или коррумпированности).

Вычисления на основе математических и логических функций в настоящее время можно произвести почти в любом табличном редакторе.

На рис. 3 показано представление условия рассматриваемой задачи, а также первый этап ее решения. Оценки в матрицах

A (в какой степени конкретному объекту O_i присущ признак P_j) и B (в какой степени каждый признак объекта P_j создает уязвимость от угрозы U_k) задаются экспертно. Оценка делается на отрезке от 0 до 1 с точностью до одной десятой. Так, например, можно видеть, что виртуальная доступность базы дынных клиентов выше, чем базы данных сотрудников: 0,7 и 0,5 в ячейках H4 и H6 соответственно).

Далее вычисления проходят по формуле, показанной на рис. 3 для ячейки с номером D22.

D22 | =($D4*D$14+$E4*D$15+$F4*D$16+$G4*D$17+$H4*D$18+$I4*D$19)/$J4

	A =		Откр.	Числ.	Частота	Физич.	Виртуал.	Коррупц.	сумма
			P_1	P_2	P_3	P_4	P_5	P_6	строки:
	БД клиентов	O_1	0,700	0,900	1,000	0,500	0,700	0,500	4,300
	БД контр.	O_2	0,500	0,700	0,300	0,700	0,800	0,500	3,500
	БД сотр	O_3	0,300	0,500	0,500	0,200	0,500	0,500	2,500
	ДБО	O_4	0,900	0,800	0,900	0,600	0,700	0,600	4,500
	СВ с контр.	O_5	0,600	0,700	0,700	0,600	0,600	0,700	3,900
	Внутр. комм.	O_6	0,100	0,300	0,300	0,200	0,600	0,900	2,400
	С. безоп.	O_7	0,000	0,300	0,400	0,200	0,200	0,800	1,900

	B =		Вредит	Вымогат	Похитит	Контраг	Персонал
			U_1	U_2	U_3	U_4	U_5
	Откр	P_1	0,700	0,700	0,900	0,500	0,000
	Числ	P_2	0,100	0,300	0,900	0,100	0,500
	Частота	P_3	0,100	0,500	0,100	0,500	1,000
	Физич	P_4	0,300	0,300	0,200	0,000	0,500
	Виртуаль	P_5	1,000	0,500	1,000	0,300	0,000
	Коррупц	P_6	0,000	0,500	0,300	0,500	1,000

			U_1	U_2	U_3	U_4	U_5
		O_1	0,356	0,467	0,579	0,326	0,512
		O_2	0,417	0,449	0,629	0,274	0,429
		O_3	0,348	0,468	0,584	0,340	0,540
	Ω =	O_4	0,373	0,478	0,582	0,331	0,489
		O_5	0,344	0,464	0,556	0,321	0,526
		O_6	0,329	0,467	0,542	0,358	0,604
		O_7	0,174	0,447	0,416	0,363	0,763

Рис. 3. Условие и первый этап решения

Для остальных ячеек формулы получаются размножением по строкам и столбцам. Размножение формул позволяет легко менять параметры модели – увеличивать число рассматриваемых объектов, вводить в матрицу новые угрозы, менять по своему усмотрению количество признаков (уменьшая для получения быстрой, но грубой оценки обстановки или увеличивая для повышения точности модели). Кстати, о точности: для получения адекватной оценки достаточно ограничиваться числами с тремя знаками после запятой, что и сделано в представленном примере. Дальнейшие вычисления приводятся на рис. 4. Матрица попарных минимумов Δ получается последовательными попарными сравнениями элементов матрицы Ω (каждый

элемент сравнивается со всеми, расположенными правее его). После этого находятся максимумы по столбцам матрицы Δ, а затем минимум из этих чисел. Это 0,34. Теперь в матрице Ω находится элемент, чуть меньший, чем 0,34. Это значение стоит в ячейке G25. Получается, что критерий δ = 0,341.

D56 =ЕСЛИ(D40<D22;D22;0)

		0,356	0,356	0,326	0,356	0,467	0,326	0,467	0,326	0,512	0,326
		0,417	0,417	0,274	0,417	0,449	0,274	0,429	0,274	0,429	0,274
		0,348	0,348	0,340	0,348	0,468	0,340	0,468	0,340	0,540	0,340
Δ =		0,373	0,373	0,331	0,373	0,478	0,331	0,478	0,331	0,489	0,331
		0,344	0,344	0,321	0,344	0,464	0,321	0,464	0,321	0,526	0,321
		0,329	0,329	0,329	0,329	0,467	0,358	0,467	0,358	0,542	0,358
		0,174	0,174	0,174	0,174	0,416	0,363	0,447	0,363	0,416	0,363
Max по столб.		0,417	0,417	0,340	0,417	0,478	0,363	0,478	0,363	0,542	0,363
Min из них		0,340									

Нахождение "чуть меньшего" элемента в матрице Ω

	U_1	U_2	U_3	U_4	U_5	
O_1	0,000	0,000	0,000	0,326	0,000	0,326
O_2	0,000	0,000	0,000	0,274	0,000	0,274
O_3	0,000	0,000	0,000	0,000	0,000	0,000
O_4	0,000	0,000	0,000	0,331	0,000	0,331
O_5	0,000	0,000	0,000	0,321	0,000	0,321
O_6	0,329	0,000	0,000	0,000	0,000	0,329
O_7	0,174	0,000	0,000	0,000	0,000	0,174

δ = 0,331

Степень угрозы (следует читать по столбцам):

	U_1	U_2	U_3	U_4	U_5
O_1	0,356	0,467	0,579	0,000	0,512
O_2	0,417	0,449	0,629	0,000	0,429
O_3	0,348	0,468	0,584	0,000	0,540
O_4	0,373	0,478	0,582	0,000	0,489
O_5	0,344	0,464	0,556	0,000	0,526
O_6	0,000	0,467	0,542	0,358	0,604
O_7	0,000	0,447	0,416	0,363	0,763

Есть угроза или нет:

	U_1	U_2	U_3	U_4	U_5
O_1	угроза	угроза	угроза	нет	угроза
O_2	угроза	угроза	угроза	нет	угроза
O_3	угроза	угроза	угроза	нет	угроза
O_4	угроза	угроза	угроза	нет	угроза
O_5	угроза	угроза	угроза	нет	угроза
O_6	нет	угроза	угроза	угроза	угроза
O_7	нет	угроза	угроза	угроза	угроза

Рис. 4. Вычисление критерия, цифровое и логическое представление ответа

Формирование ответа показано на примере ячейки D56. Угроза признается существенной, если значение в ячейке больше или равно значению критерия.

Как видно из приведенного примера (ячейка H62), наибольшую угрозу системе безопасности банка представляют собственные сотрудники (возможно, вследствие избыточных прав доступа сотрудников к секретной информации или нездоровой обстановки в коллективе, создающей условия для потенциальной коррупции).

О реорганизации подразделений с учетом оценки внешних угроз

Отметим, что в быстро меняющихся условиях, в которых функционирует современная банковская система, для каждой кредитной организации важнейшее значение приобретает оценка внешних угроз, и в первую очередь рисков, связанных с

нелегитимными действиями западных стран, продемонстрировавших способность в одностороннем порядке по политическим причинам частично или полностью заблокировать, а в перспективе – конфисковать банковские активы (финансы, недвижимость и т. д.) на своей территории. Нет сомнений в том, что для предупреждения подобных угроз и преодоления их последствий руководство отдельно взятого банка не может принять исчерпывающих мер, однако оценка уровня их опасности и проработка действий по реагированию на них (в первую очередь по маневрированию ресурсами) ложатся в первую очередь на высший менеджмент кредитно-финансовой организации. По этой причине вовлеченность руководства банка в работу органов безопасности неизбежно должна возрасти, и это необходимо отразить в структуре этих органов, в схеме соподчиненности и ответственности подразделений банка.

И это касается не только руководства. Значительная часть угроз и рисков банковской деятельности может быть существенно уменьшена при формировании оптимальных организационных структур коммерческого банка, основных функциональных обязанностей его работников, сориентированных на обеспечение безопасности. Специальные знания и практические навыки персонала способствуют более конкретному представлению о внутренних механизмах взаимодействия отдельных управлений (департаментов) коммерческого банка, об организации документооборота по отдельным банковским операциям, что становится все более очевидным по мере развития цифровых технологий [4. – С. 87].

Для гибкого реагирования на динамично меняющиеся условия среды современному банку нужно быть готовым к быстрой реорганизации структурных подразделений, к изменению круга задач, стоящих перед ними, а при необходимости – к введению ограничений на выполнение некоторых функций или доступ к определенной информации для подразделений и отдельных сотрудников.

В частности, в настоящее время юридическое управление банка занимается следующими видами деятельности:

– принимает участие в разработке новых уставных и иных нормативных документов банка;

– контролирует оформление сделок и исполнение уставных положений;

– стандартизирует и формирует договоры по различным банковским операциям;

– обслуживает ведение дел банка в учреждениях, органах исполнительной власти, а также в судах;

– делает заключения по разнообразным юридическим вопросам, связанным с деятельностью банка.

В силу доступа специалистов этого управления к конфиденциальным данным, связанным с различными сферами деятельности коммерческого банка, на первый взгляд целесообразно ограничивать их доступ к таким материалам, как:

– договорные дела – договоры и соглашения, сопроводительные документы, протоколы и дополнительные соглашения к договорам по всем видам деятельности банка;

– учетные, поисковые и справочные журналы, картотеки, базы данных по договорам;

– документы, сопровождающие претензионную и исковую работу;

– предложения по результатам анализа результатов финансово-хозяйственной деятельности;

– сведения о содержании и ходе переговоров с партнерами, акционерами, клиентами и иными юридическими и физическими лицами;

– данные о платежеспособности клиентов и партнеров банка, их производственной, торговой и иной хозяйственной деятельности;

– перечни (списки полные и выборочные) акционеров банка;

– сведения, раскрывающие особые условия заключенных контрактов в части скидок, процентных ставок, рассрочки платежей и т. д.;

– сводная информация об участии в качестве учредителя акционерных и совместных предприятий, дочерних банков, иных коммерческих структур, о размере капитала в уставном фонде;

– реестр регистрации выдачи акций;

– журнал регистрации договоров и соглашений.

С другой стороны, по итогам оценки уровня внешних угроз подобные ограничения следует вводить выборочно с учетом конкретной обстановки.

Организатором и координатором всей деятельности банка в области безопасности является служба безопасности банка, структуру которой, как правило, образуют сектора – охраны, режима, технической защиты и экономической безопасности. На фоне возрастающей угрозы применения искусственного интеллекта (ИИ) при осуществлении хищений средств банка или обеспечении мошеннических схем перед современным банком возникает новая задача – повышение уровня безопасности в этой сфере с опорой на собственные уникальные алгоритмы искусственного интеллекта, отражающие специфику и уникальность операций конкретного банка. С этой целью руководству банка уже сейчас имеет смысл задуматься о создании принципиально нового сектора – ИИ (по аналогии с тем, как решается эта проблема уже во многих государственных организациях) [3. – С. 66].

Основными направлениями деятельности сектора охраны являются обеспечение физической безопасности зданий, офисов, оборудования, сотрудников, проводимых мероприятий, перевозок.

Деятельность сектора режима сосредоточена на обеспечении секретности документов, организации режима допуска и контроля посетителей.

Работа сектора технической защиты состоит в обнаружении технических каналов утечки информации и несанкционированного доступа к ней, поддержании в рабочем состоянии систем видеонаблюдения, сигнализации и связи, а также проведении противопожарных мероприятий.

Основными направлениями деятельности сектора экономической безопасности являются изучение и анализ преступных действий в финансовой сфере, мониторинг поведения конкурентов, исследование и учет попыток проникновения в секреты банка, выявление возможных слабых мест в деятельности банка.

Важным фактором надежной работы служб безопасности коммерческих банков остается их тесное взаимодействие с правоохранительными органами по собственной инициативе и вследствие ориентировок, поступающих от них.

Наконец, как и другие подразделения коммерческого банка, служба безопасности должна предпринимать постоянные усилия по обеспечению сохранности любой информации, связанной непосредственно с обеспечением деятельности в сфере безопасности банковской деятельности, включая:

– нормативные и организационные документы по защите государственной, служебной и банковской тайны;

– положение о службе безопасности;

– инструкцию о пропускном режиме в банке;

– методику подбора персонала;

– проектные и эксплуатационные документы по инженерно-технической защите выделенных помещений;

– документы по инженерно-технической и программной защите информации в средствах вычислительной техники;

– должностные инструкции сотрудников службы безопасности;

– договоры и сопроводительные документы по функционированию комплексной системы защиты информации;

– переписку и переговоры по вопросам защиты информации;

– инструкцию по обработке и хранению документов, содержащих банковскую тайну;

– инструкцию по охране помещений и персонала банка.

Естественно, свою специфическую структуру может иметь и средний по величине капитала акционерный коммерческий банк, который наиболее часто может выступать как партнер для средних и малых торговых предприятий. Так, например, вместо крупного юридического управления в среднем банке может функционировать только небольшой аналогичный по функциям отдел. Количество управлений в самом банке может быть существенно меньше, чем в крупном.

Заключение

Как видим, реализация безопасной банковской деятельности требует постоянных усилий со стороны всех работников коммерческого банка. Важно заметить, что сами угрозы носят комплексный характер, зависят от ряда динамично меняющихся факторов и требуют с учетом результатов адекватных моделей, построенных на основе регулярно обновляющихся данных, применения комплексного подхода к разработке программ безопасного функционирования коммерческого банка.

В настоящее время важнейшее значение приобретает оценка внешних угроз. Для их предупреждения действий руководства отдельного банка недостаточно, однако оценка уровня их опасности и проработка мер по реагированию на них (в первую очередь маневрированию ресурсами) лежит на высшем менеджменте кредитно-финансовой организации. Поэтому структуру органов управления, схему соподчиненности и ответственности подразделений банка следует изменить в целях повышения вовлеченности руководства банка в работу органов безопасности, в том числе с применением собственных алгоритмов ИИ.

Значительная часть угроз и рисков банковской деятельности может быть существенно уменьшена при формировании оптимальных организационных структур коммерческого банка, основных функциональных обязанностей его работников, сориентированных на обеспечение безопасности.

Список литературы

1. *Борисов В. Р.* Экономическая безопасность в информационной среде и банковские мошенники // Инновационное развитие экономики. – 2021. – № 4. – С. 223–229.

2. *Васильева Ю. А., Цыганова М. В.* Надежность и безопасность как составляющие качества банковских услуг и факторы конкурентоспособности банков // Проблемы экономики и юридической практики. – 2018. – № 5. – С. 92–98.

3. *Ващекин А. Н., Ващекина И. В.* Искусственный интеллект в судебной системе: задачи и методы // Правовая информатика. – 2023. – № 3. – С. 86–95.

4. *Ващекин А. Н., Ващекина И. В.* Противодействие преступной деятельности в условиях развития цифровых технологий дистанционного банковского обслуживания // Правовая информатика. – 2019. – № 4. – С. 65–74.

5. *Велингурский В. А., Белозерова Г. И., Федосеев С. В.* Построение и реализация модели оценки уровня мошеннических операций в банке-эквайре на основе самоорганизующейся карты Кохонена // Информационные технологии в процессе подготовки современного специалиста. – Липецк, 2016. – С. 24–32.

6. *Виноградова А. С., Молчанов И. Н.* Подходы к обеспечению информационной безопасности банковского сектора // Теория и практика проектного образования. – 2020. – № 2. – С. 40–42.

7. *Губайдуллина И. Н.* Основные направления деятельности подразделений банковской безопасности // Сегодня и завтра российской экономики. – 2018. – № 87-88. – С. 61–68.

8. *Гугнюк К. М., Гугнюк И. Г.* Банковская безопасность как элемент обеспечения финансовой безопасности государства // Вестник Саратовской государственной юридической академии. – 2022. – № 1. – С. 231–237.

9. *Кузовлева Н. Ф., Тарасова Н. В.* Цифровизация банковской сферы: тенденции развития и экономическая безопасность // Экономика и управление: проблемы, решения. – 2021. – Т. 9. – № 1. – С. 93–98.

10. *Курманова Л. Р., Галимарданов А. Р.* Проблемные аспекты экономической безопасности в банковской системе России // Инновационное развитие экономики. – 2020. – № 2. – С. 260–289.

11. *Ловцов Д. А.* Принципы обеспечения защищенности информации в эргасистемах // Правовая информатика. – 2021. – № 1. – С. 36–50.

12. *Лосев В. С., Пяткова Е. А.* Моделирование рисков банковской деятельности и информационной безопасности // Вестник Тихоокеанского государственного университета. – 2019. – № 1. – С. 99–108.

13. *Приходько К. А.* Применение закона № 187-ФЗ «О безопасности критической информационной структуры Российской Федерации» организацией, осуществляющей деятельность в банковской сфере // Актуальные научные исследования в современном мире. – 2021. – № 5-2. – С. 153–157.

14. *Саати Т. Л.* Принятие решений. Метод анализа иерархий. – М. : Радио и связь, 1993.

15. *Хубулава Н. М., Скотченко, А. С.* Модель возможности деноминационной политики национальной валюты в условиях коронавирусной инфекции // Russian Economic Bulletin. – 2021. – Т. 4. – № 4. – С. 262–267.

16. *Чаплыгина А. В.* Экономическая безопасность банковской деятельности // NovaUm.Ru. – 2017. – № 10. – С. 114–115.

17. *Черная Е. Г.* Финансовая безопасность коммерческого банка как фактор обеспечения его экономической безопасности // Вестник ВИЭПП. – 2021. – № 1. – С. 73–76.

18. *Черняков С. А.* Преступность в сфере банковских отношений: тенденции развития // Известия Юго-Западного государственного университета. Серия: История и право. – 2019. – Т. 3. – № 9. – С. 95–103.

19. *Mukusheva A. G., Zholamanova M. T., Kuchukova, N. K.* Financial Technologies in the Banking Sector: Prospects and Security // Bulletin of Karaganda University, Economy Series. – 2021. – N 1 (101). – P. 92–102.

20. *Zadeh L. A.* Fuzzy Sets // Information and Control. – 1965. – N 8. – P. 338–353.

21. *Zoidov K. H., Rahmatova Z. I., Zoidov Z. K.* Modeling the Impact of Uneven External Threats on the Economic Security of the Russian Banking System in Conditions of Instability // Scientofoc Review. Vol. 1: Economics and Law. – 2018. – N 6. – P. 236–254.

References

1. Borisov V. R. Ekonomicheskaya bezopasnost v informatsionnoy srede i bankovskie moshenniki [Economic Security in the Information Environment and Banking Scammers]. *Innovatsionnoe razvitie ekonomiki* [Innovative Development of the Economy], 2021, No. 4, pp. 223–229. (In Russ.).

2. Vasileva Yu. A., Tsyganova M. V. Nadezhnost i bezopasnost kak sostavlyayushchie kachestva bankovskikh uslug i faktory konkurentosposobnosti bankov [Reliability and Security as Components of the Quality of Banking Services and Factors of Competitiveness of Banks].

Problemy ekonomiki i yuridicheskoy praktiki [Problems of Economics and Legal Practice], 2018, No. 5, pp. 92–98. (In Russ.).

3. Vashchekin A. N., Vashchekina I. V. Iskusstvennyy intellekt v sudebnoy sisteme: zadachi i metody [Artificial Intelligence in the Judicial System: Tasks and Methods]. *Pravovaya informatika* [Legal Informatics], 2023, No. 3, pp. 86–95. (In Russ.).

4. Vashchekin A. N., Vashchekina I. V. Protivodeystvie prestupnoy deyatelnosti v usloviyakh razvitiya tsifrovykh tekhnologiy distantsionnogo bankovskogo obsluzhivaniya [Countering Criminal Activity in the Context of the Development of Digital Technologies for Remote Banking Services]. *Pravovaya informatika* [Legal Informatics], 2019, No. 4, pp. 65–74. (In Russ.).

5. Velingurskiy V. A., Belozerova G. I., Fedoseev S. V. Postroenie i realizatsiya modeli otsenki urovnya moshennicheskikh operatsiy v banke-ekvayre na osnove samoorganizuyushcheysya karty Kokhonena [Construction and Implementation of a Model for Assessing the Level of Fraudulent Transactions in an Acquiring Bank Based on a Self-Organizing Kohonen Map]. *Informatsionnye tekhnologii v protsesse podgotovki sovremennogo spetsialista* [Information Technology in the Process of Training a Modern Specialist]. Lipetsk, 2016, pp. 24–32. (In Russ.).

6. Vinogradova A. S., Molchanov I. N. Podkhody k obespecheniyu informatsionnoy bezopasnosti bankovskogo sektora [Approaches to Ensuring Information Security of the Banking Sector]. *Teoriya i praktika proektnogo obrazovaniya* [Theory and Practice of Project Education], 2020, No. 2, pp. 40–42. (In Russ.).

7. Gubaydullina I. N. Osnovnye napravleniya deyatelnosti podrazdeleniy bankovskoy bezopasnosti [The Main Activities of Banking Security Units]. *Segodnya i zavtra rossiyskoy ekonomiki* [Today and Tomorrow of the Russian Economy], 2018, No. 87-88, pp. 61–68. (In Russ.).

8. Gugnyuk K. M., Gugnyuk I. G. Bankovskaya bezopasnost kak element obespecheniya finansovoy bezopasnosti gosudarstva [Banking Security as an Element of Ensuring the Financial Security of the State]. *Vestnik Saratovskoy gosudarstvennoy yuridicheskoy akademii* [Bulletin of the Saratov State Law Academy], 2022, No. 1, pp. 231–237. (In Russ.).

9. Kuzovleva N. F., Tarasova N. V. Tsifrovizatsiya bankovskoy sfery: tendentsii razvitiya i ekonomicheskaya bezopasnost [Digitalization of the Banking Sector: Development Trends and Economic Security]. *Ekonomika i upravlenie: problemy, resheniya* [Economics and Management: Problems, Solutions], 2021, Vol. 9, No. 1, pp. 93–98. (In Russ.).

10. Kurmanova L. R., Galimardanov A. R. Problemnye aspekty ekonomicheskoy bezopasnosti v bankovskoy sisteme Rossii [Problematic Aspects of Economic Security in the Banking System of Russia]. *Innovatsionnoe razvitie ekonomiki* [Innovative Development of the Economy], 2020, No. 2, pp. 260–289. (In Russ.).

11. Lovtsov D. A. Printsipy obespecheniya zashchishchennosti informatsii v ergasistemakh [Principles of Ensuring the Security of Information in Ergasystems]. *Pravovaya informatika* [Legal Informatics], 2021, No. 1, pp. 36–50. (In Russ.).

12. Losev V. S., Pyatkova E. A. Modelirovanie riskov bankovskoy deyatelnosti i informatsionnoy bezopasnosti [Modeling the Risks of Banking and Information Security]. *Vestnik Tikhookeanskogo gosudarstvennogo universiteta* [Pacific State University Bulletin], 2019, No. 1, pp. 99–108. (In Russ.).

13. Prikhodko K. A. Primenenie zakona № 187-FZ «O bezopasnosti kriticheskoy informatsionnoy struktury Rossiyskoy Federatsii» organizatsiey, osushchestvlyayushchey deyatelnost v bankovskoy sfere [Application of Law No. 187-FZ "On the Security of the Critical Information Structure of the Russian Federation" by an organization operating in the banking

sector]. *Aktualnye nauchnye issledovaniya v sovremennom mire* [Actual Scientific Research in the Modern World], 2021, No. 5-2, pp. 153–157. (In Russ.).

14. Saati T. L. Prinyatie resheniy. Metod analiza ierarkhiy [Decision Making. Hierarchy Analysis Method]. Moscow, Radio and Communications, 1993. (In Russ.).

15. Khubulava N. M., Skotchenko, A. S. Model vozmozhnosti denominatsionnoy politiki natsionalnoy valyuty v usloviyakh koronavirusnoy infektsii [Model of the Possibility of the Denomination Policy of the National Currency in the Conditions of the Coronavirus Infection]. *Russian Economic Bulletin*, 2021, Vol. 4, No. 4, pp. 262–267. (In Russ.).

16. Chaplygina A. V. Ekonomicheskaya bezopasnost bankovskoy deyatelnosti [Economic Security of Banking]. *NovaUm.Ru*, 2017, No. 10, pp. 114–115. (In Russ.).

17. Chernaya E. G. Finansovaya bezopasnost kommercheskogo banka kak faktor obespecheniya ego ekonomicheskoy bezopasnosti [Financial Security of a Commercial Bank as a Factor in Ensuring its Economic Security]. *Vestnik VIEPP* [VIEPP Bulletin], 2021, No. 1, pp. 73–76. (In Russ.).

18. Chernyakov S. A. Prestupnost v sfere bankovskikh otnosheniy: tendentsii razvitiya [Crime in Banking Relations: Development Trends]. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Seriya: Istoriya i parvo* [Proceedings of the Southwestern State University, Series: History and Law], 2019, Vol. 3, No. 9, pp. 95–103. (In Russ.).

19. Mukusheva A. G., Zholamanova M. T., Kuchukova, N. K. Financial Technologies in the Banking Sector: Prospects and Security. *Bulletin of Karaganda University, Economy Series,* 2021, No. 1 (101), pp. 92–102.

20. Zadeh L. A. Fuzzy Sets. *Information and Control*, 1965, No. 8, pp. 338–353.

21. Zoidov K. H., Rahmatova Z. I., Zoidov Z. K. Modeling the Impact of Uneven External Threats on the Economic Security of the Russian Banking System in Conditions of Instability. *Scientofoc Review. Vol. 1: Economics and Law*, 2018, No. 6, pp. 236–254.

Сведения об авторах

Ирина Викторовна Ващекина
кандидат экономических наук, доцент,
доцент кафедры информационного права,
информатики и математики
Российского государственного университета
правосудия.
Адрес: ФГБОУ ВО «Российский
государственный университет правосудия»,
117418, Москва, Новочеремушкинская ул., д. 69.
E-mail: vaschekina@mail.ru

Андрей Николаевич Ващекин
кандидат экономических наук, доцент,
профессор кафедры информационного права,
информатики и математики
Российского государственного университета
правосудия.
Адрес: ФГБОУ ВО «Российский
государственный университет правосудия»,
117418, Москва, Новочеремушкинская ул., д. 69.
E-mail: vaschekin@mail.ru

Information about the authors

Irina V. Vashchekina
PhD, Assistant Professor,
Assistant Professor of the Department
for Information Law, Computer Science
and Mathematics of the Russian State
University of Justice.
Address: Russian State University of Justice,
69 Novocheremushkinskaya Str.,
Moscow, 117418, Russian Federation.
E-mail: vaschekina@mail.ru

Andrei N. Vashchekin
PhD, Assistant Professor,
Professor of the Department
for Information Law, Computer Science
and Mathematics of the Russian State
University of Justice.
Address: Russian State University of Justice,
69 Novocheremushkinskaya Str.,
Moscow, 117418, Russian Federation.
E-mail: vaschekin@mail.ru