Azimut of Scientific Research: Economics and Administration.
2021. Т.10. №3(36) *p-ISSN: 2309-1762; e-ISSN: 2712-8482*

УДК 336.71
DOI: 10.26140/anie-2021-1003-0074

ФОРМИРОВАНИЕ ТЕХНОЛОГИИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ БАНКОВСКОЙ ДЕЯТЕЛЬНОСТИ В СОВРЕМЕННЫХ УСЛОВИЯХ

SPIN: 3283-7501
AuthorID: 570195
ORCID: 0000-0002-7211-66-14
САДЫКОВА Люция Мунировна, кандидат экономических наук, доцент,
доцент кафедры «Банковское дело и страхование»
Оренбургский государственный университет
(460018, Россия, Оренбург, улица Терешкова, 10/2-37, e-mail: sad.l.m@mail.ru)
SPIN: 9361-8823
AuthorID: 555136
ORCID: 0000-0003-0325-4180
КОРОБЕЙНИКОВА Елена Владимировна, кандидат экономических наук,
доцент кафедры «Национальная и мировая экономика»
Самарский государственный технический университет
(443030, Россия, Самара, улица Мечникова 50 «А»-11, e-mail: korob-lena-79@mail.ru)

Аннотация. В работе исследуются теоретические и практические аспекты формирования и развития технологии обеспечения безопасности банковской деятельности в России в современных условиях. Авторами предпринята попытка выявить потенциальные угрозы, способные нанести ущерб законным интересам банка и определить необходимость развития технологий обеспечения безопасности банковской деятельности. В статье определены основные структурные компоненты технологии обеспечения безопасности банковской деятельности, выделены объекты и субъекты правоотношений в сфере безопасности коммерческого банка. Авторами проведен анализ ключевых угроз в области защищенности внутренней банковской сети, защищенности онлайн-банкинга, проведена оценка изменения уязвимостей банковского бизнеса различного уровня риска, а также практики применения технологий обеспечения безопасности банковской деятельности в российских банках. На основе проведенного анализа авторами были выявлены наиболее значимые проблемы обеспечения безопасности банков, определены задачи, а также основные направления по совершенствованию и внедрению перспективных технологий обеспечения безопасности банковской деятельности, исходя из формируемой стратегии обеспечения безопасности банка.

Ключевые слова: экономическая безопасность**,** технологии обеспечения безопасности банковской деятельности, факторы и угрозы экономической безопасности банка, несанкционированные операции, уровень риска, уровень защищенности, противоправные финансовые операции, стратегия развития банка.

FORMATION OF TECHNOLOGY TO ENSURE THE SECURITY OF BANKING ACTIVITIES IN MODERN CONDITIONS

SADYKOVA Lucia Munirovna, candidate of economic sciences, associate professor,
associate professor of the Department of «Banking and insurance»
Orenburg State University
(460018, Russia, Orenburg, Tereshkova street, 10/2-37, e-mail: sad.l.m@mail.ru)
KOROBEYNIKOVA Elena Vladimirovna, candidate of economic sciences,
associate professor of the Department of «National and world economy»
Samara State Technical University
(443030, Russia, Samara, Mechnikova street,50 «A»-11, e-mail: korob-lena-79@mail.ru)

Abstract. The paper discusses the theoretical and practical aspects of the formation and development of technology to ensure the security of banking activities in Russia in modern conditions. The authors made an attempt to identify potential threats that could damage the legitimate interests of the bank and determine the need for the development of technologies to ensure the security of banking activities. The article identifies the main structural components of the technology for ensuring the security of banking activities, identifies the objects and subjects of legal relations in the field of security of a commercial bank. The authors analyzed the key threats in the field of security of the internal banking network, security of online banking, assessed changes in the vulnerabilities of the banking business of various levels of risk, as well as the practice of applying banking security technologies in Russian banks. Based on the analysis, the authors identified the most significant problems of ensuring the security of banks, identified the tasks, as well as the main directions for improving and introducing promising technologies for ensuring the security of banking activities, based on the formed strategy for ensuring the security of the bank.

Keywords: economic security, technologies for ensuring the security of banking activities, factors and threats to the economic security of a bank, unauthorized operations, level of risk, level of security, illegal financial transactions, bank development strategy.

ВВЕДЕНИЕ

Необходимость проведения мероприятий по безопасности в управленческой, экономической и правовой сферах деятельности, которые непосредственно взаимосвязаны между собой, определяют важность безопасности всей банковской деятельности.

Актуальность данного исследования определяет то, что технологии обеспечения безопасности банковской деятельности необходимы для защиты интересов банка от реальных или потенциальных угроз со стороны физических и юридических лиц, вследствие которых могут произойти потери банковских ресурсов.

Поддерживать безопасность собственной деятельности на высоком уровне во всех направлениях своего развития помогает и обеспечивает система безопасности банка. При этом, к основным направлениям обеспечения безопасности банковской деятельности следует отнести: экономическую, финансовую, кадровую, интеллектуальную, информационную, физическую, инновационную и экологическую безопасность.

МЕТОДОЛОГИЯ

Целью исследования является анализ и выявление

тенденций развития технологий обеспечения безопасности банковской деятельности. Достижение поставленной цели возможно при выполнении следующих задач: исследование общих понятий технологий обеспечения безопасности банковской деятельности, выявление необходимости их развития, проведение анализа практического использования технологий обеспечения безопасности банковской деятельности российскими кредитными организациями и определение совокупности мероприятий по совершенствованию и внедрению перспективных технологий обеспечения безопасности банковской деятельности.

Методологическую основу составляет комплексный анализ показателей угроз обеспечения безопасности банков, что позволит выявить ключевые тенденции развития технологий обеспечения безопасности банковской деятельности.

Развитие технологий обеспечения безопасности банковской деятельности привлекает интерес множества отечественных и зарубежных исследователей. В частности, вопросы общей теории экономической безопасности кредитных организаций исследуют такие отечественные ученые как: Л.И. Абалкин, С.Ю. Глазьев, В.С. Загашвили, О.И. Лаврушин, Н.Н. Потрубач, В.К. Сенчагов и другие авторы. Вместе с тем, современные тенденции, связанные с развитием и масштабированием цифровых технологий, с увеличением доли онлайн операций, свидетельствуют о необходимости развития научно обоснованной системы взглядов на определение основных направлений, условий и порядка практического решения задач формирования и развития технологий обеспечения безопасности банковской деятельности с целью формирования защиты банковского дела от возможных противоправных действий.

РЕЗУЛЬТАТЫ

Объектами правоотношений в сфере безопасности коммерческого банка выступают его персонал, информация, материальные ценности, финансы, новейшие технологии. Основными субъектами таких правоотношений являются органы государственной власти, Центральный банк РФ, непосредственно коммерческий банк, служба безопасности коммерческого банка, его контрагенты [1].

Регулятором всех отношений в банковской сфере, в том числе и ее безопасности, является государство, которое обеспечивает эту безопасность на государственном уровне [2]. Безопасность всего банковского коммерческого сектора, проведение денежно-кредитной политики обеспечивает ЦБ РФ, который также осуществляет и регулирование безопасности деятельности банков [3]. Коммерческий банк, как собственник ресурсов, представляющих коммерческую, банковскую и служебную тайну, а также являющийся субъектом правоотношений в сфере безопасности, должен обеспечивать безопасность данных. Стоит отметить, что для собственной безопасности банки могут помимо штатной службы безопасности использовать и частные охранно-детективные структуры.

В качестве основных объектов защиты технологий обеспечения безопасности банковской деятельности следует выделить персонал банка, информационные ресурсы, банковские документы, финансовые средства, информационные системы и технологии, пользовательские права на получение безопасных информационных услуг [4]. Основными компонентами системы технологий обеспечения безопасности банковской деятельности являются предотвращение, обнаружение, и реагирование на возможные угрозы обеспечения безопасности банковской деятельности.

Таким образом, под безопасностью банка следует понимать состояние защищенности интересов его владельцев, руководства и клиентов, материальных ценностей и информационных ресурсов от внутренних и внешних угроз [5]. На технологию обеспечения безопасности деятельности банка существенное влияние оказывают:

- преступные группировки;
- уровень развития теневой экономики;
- противоправные финансовые операции;
- угрозы насильственного характера над персоналом;
- покушения и ограбления;
- недостаточная лояльность персонала и его квалификация,
- недостаток финансовых ресурсов и др.

Технологии обеспечения безопасности банковской деятельности являются структурной единицей государственной экономической безопасности, поскольку банковская деятельность оказывает непосредственное влияние на финансовую стабильность государства [6]. Обеспечение банковской безопасности возложено на учредителей банка, исполнительные органы и государство. В силу постоянно изменяющихся условий коммерческим банкам необходимо регулярно заниматься развитием данных технологий безопасности. Формирование перечня необходимых технологий для обеспечения безопасности банковской деятельности осуществляется на уровне концепции экономической безопасности, которая должна свести к минимуму опасности, риски и угрозы посредством решения конкретных задач. От качества их проработанности зависит эффективность банковской системы безопасности.

С целью своевременного выявлении угроз технология организации безопасности банковской деятельности должна способствовать контролю над всеми сферами деятельности банка и его конкретными операциями. Наличие огромного числа факторов возникновения банковских рисков определяет необходимость их нивелирования и формирования технологии, включающей: выявление фактора появления угрозы (риска), анализ выявленной угрозы, определение необходимости борьбы с выявленной угрозой и определение методов борьбы с ней.

Классификация технологий обеспечения безопасности банковской деятельности напрямую связана с тем, какие именно угрозы они должны нейтрализовать. Угрозы безопасности банка разнообразны. Так, в частности, по природе возникновения угрозы могут быть: политические, правовые, экономические, конкурентные, контрагентские, техногенные, криминальные, экологические и др. По вероятности возникновения следует выделить явные и скрытые угрозы, по результатам влияния – общие и локальные угрозы. По отношению угроз безопасности к деятельности человека они бывают субъективные, которые обусловлены человеческой деятельностью, и объективные, которые возникают в результате стихийных природных явлений. Совокупность всех угроз безопасности банка, можно классифицировать на внешние и внутренние [7]. Эта классификация обусловлена, факторами, которые их порождают. С целью принятия оперативных решений по борьбе с возникающими угрозами безопасности банка руководство банка и служба безопасности должны постоянно контролировать изменения внешних и внутренних факторов и их динамику. Анализ и дальнейшая оценка этих угроз должна быть оперативной и адекватной. Именно благодаря данным полученным в ходе этой оценки у банка появится возможность разработать план по противодействию угрозам безопасности, заранее предотвратить посягательства мошенников и дать ответную реакцию на негативное рыночное воздействие.

Анализ угроз безопасности банка, как правило, обеспечивается службой его безопасности. Данное структурное подразделение, образуемое руководством банка, должно обеспечивать стабильную дея-

Azimut of Scientific Research: Economics and Administration.
2021. Т.10. №3(36) *p-ISSN: 2309-1762; e-ISSN: 2712-8482*

тельность всех компонентов, среди которых экономические, финансовые, технические, кадровые, правовые, коммерческие, режимные и прочие компоненты. Стоит отметить, что служба безопасности проводит свою деятельность непосредственно в соответствии с документацией, утвержденной банком, а именно с уставом и инструкцией. В данных документах прописаны цель, задачи службы безопасности, а также обязанности и ее права. Обнаружение, нейтрализация угроз безопасности и причин их возникновения являются основной целью службы безопасности. Задачи этой службы разноплановы, это прежде всего защита имущества, конфиденциальной информации банка и обеспечение безопасности персонала и др. [8].

Обзор технологий обеспечения безопасности банковской деятельности в России показал следующее. Увеличение количества компьютерных преступлений в банковской сфере носит глобальный характер, данная ситуация требует сплоченных и скоординированных усилий всех регуляторов, а также правоохранительных органов и непосредственно самих кредитно-финансовых организаций и потребителей их услуг.

По итогам 2020 г. в России объем проведенных несанкционированных операций со счетов юридических лиц составил 1,469 млрд. руб., тогда как в предыдущем году – 1,57 млрд. руб., в 2018 г. и 2017 г. порядка 1,89 млрд. руб. и 1,37 млрд. руб. соответственно. Несанкционированных операций с использованием платежных карт, выпущенных российскими кредитными организациями в 2020 г. было проведено на сумму 1,384 млрд. руб. За предыдущие года данный показатель составил в 2019 г. - 0,961 млрд. руб., в 2018 г. - 1,08 млрд. руб., в 2017 г. - 1,14 млрд. руб. Доля данных операций в совокупном объеме операций с использованием платежных карт, выпущенных кредитными организациями России по окончанию 2020 г. составила 0,0018 % или 1,8 коп. на 1000 руб. переводов. Стоит отметить, что Европейская служба банковского надзора (EBA) устанавливает лимит допустимого удельного веса несанкционированных переводов денежных средств, который составляет 5 евроцентов на 1000 евро переводов [9].

В 2019 году Банк России принял первый стратегический документ: «Основные направления развития информационной безопасности кредитно-финансовой сферы на период 2019–2021 годов», в котором определены основные приоритеты по обеспечению безопасности банковской деятельности на ближайшее время, а именно:

-создание риск-профилей финансовых организаций и переход к риск-ориентированному надзору,

-введение требований к устойчивости и бесперебойности деятельности финансовых организаций при реализации киберрисков,

-требования к безопасности управления данными и предотвращение утечек данных из финансовых организаций,

-развитие киберкультуры финансового рынка.

Большинство федеральных банков движется в направлении принятого стандарта Банка России по информационной безопасности. При этом 41,7 % банков уже внедрили некоторые положения стандарта, а еще 40,8 % приняли решение об их реализации в ближайшем будущем [10]. По итогам 2018 и 2019 годов кредитно-финансовые организации входят в число наиболее атакуемых: они входят в топ-3 по общему количеству проведенных атак [11]. Главный мотив злоумышленников - получение финансовой выгоды (65 % инцидентов в 2019 г. и 92 % - в 2018 г.). Доля инцидентов, нацеленных на получение информации о платежных картах, персональных данных, учетных данных пользователей для доступа к личным кабинетам, с 2018 по 2019 год увеличилась с 8 % до 31 % (рисунок 1) [12].

Рисунок 1 – Основные мотивы атак на кредитные организации

Безопасность внутренних сетей кредитных организаций далека от совершенства. Типовые векторы атак во внутренней сети часто базируются на слабой парольной политике и недостаточной защите от восстановления паролей из памяти оперативных систем (рисунок 2) [2].

Рисунок 2 – Основные виды недостатков и уязвимостей внутренней сети банков

Почти в 50 % систем слабые пароли устанавливают пользователи, но чаще используются стандартные учетные записи, оставляемые администраторами при установке СУБД, веб-серверов, ОС или создании служебных учетных записей.

К числу ключевых тенденций 2019 года в области защищенности онлайн-банкинга относится сокращение доли уязвимостей высокого уровня риска с 32 % в 2018 г. до 15 % в 2019 г. (рисунок 3) [12].

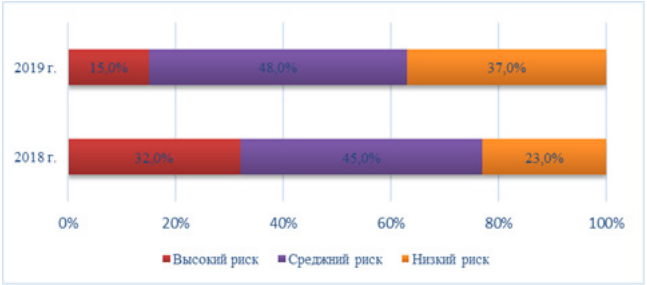

Рисунок 3 – Доля уязвимостей различного уровня риска банков

В мобильных приложениях уязвимости высокого уровня риска обнаружены в 38 % приложений для IOS и 43% приложений для платформ под управлением Android, в 2018 г. уязвимости такого типа обнаружены в 25 % и 56% приложений соответственно (рисунок 4) [12].

OECD: 5.02 Economics and business; ASJC: 2000; WoS Subject Categories: GY, PC

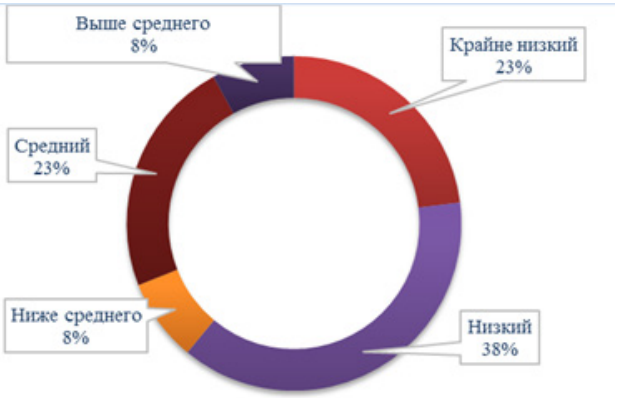

Рисунок 4 – Уровень защищенности онлайн-банков, доля систем

Большинство проблем безопасности - общие для обеих платформ. Небезопасное хранение данных - основной недостаток, он выявлен в 76% мобильных приложений, что на 11% выше показателя 2018 г. Под угрозу попадают пароли, финансовая информация и персональные данные пользователей. Значительно сократить время присутствия злоумышленников в инфраструктуре и предотвратить достижение поставленных ими целей помогает анализ трафика и событий, профилирование действий пользователей и возможность исследования оперативной памяти, процессов и др. Однако стоит отметить, что средства защиты будут давать неэффективные результаты без поддержки высококвалифицированных специалистов в области расследования инцидентов.

Следует отметить, что перспективы развития технологий обеспечения безопасности банковской деятельности должны определяться совокупностью задач их развития. Проведенный анализ свидетельствует о необходимости и целесообразности разработки собственной системы безопасности банка, которая может быть выстроена в соответствии с одной из трех стратегий [13].

Первая стратегия безопасности может быть ориентирована на решение уже существующих проблем. В рамках данной стратегии банк обязан возмещать, восстанавливать и проводить компенсацию уже произошедших потерь. При использовании данной стратегии банку сложно осуществлять свою деятельность, есть большие риски, что банк будет закрыт, поэтому применение данной стратегии не приветствуется. Ее применение возможно в условиях восполнения причиненного ущерба.

Более прогрессивной является вторая стратегия безопасности банка. Ее ориентация проводится на молниеносную реакцию банка на любую возникшую угрозу, такую стратегию называют «угроза-отражение». Данную стратегию сложно считать совершенной, но все же ее использует большинство банков. Для ее реализации в структуре банка создаются специализированные подразделения, деятельность которых направлена на предотвращение или ослабление угроз.

Наиболее прогрессивной является третья стратегия. Планирование и прогнозирование являются главными составляющими данной стратегии, поскольку структурные подразделения банков занимаются выявлением различного вида угроз на ранних стадиях, задолго до оказания их негативного влияния. В соответствии с планами и прогнозами у банка есть время на подготовку к предстоящим угрозам, что обеспечивает ликвидацию этих угроз с наименьшими потерями. Рассматриваемая стратегия безопасности применяется прогрессивно развивающимися банками.

В соответствии с Информацией Банка России от 28 сентября 2020 г. «Основные направления развития информационной безопасности кредитно-финансовой сферы на период 2019-2021 годов» определены основные цели и задачи развития информационной безопасности и киберустойчивости, среди которых следует выделить [14]:

- необходимость обеспечения информационной безопасности и киберустойчивости для обеспечения финансовой стабильности организаций финансового рынка;
- необходимость обеспечения операционной надежности и непрерывности деятельности организаций кредитно-финансовой сферы;
- обеспечение противодействия компьютерным атакам, в том числе при использовании инновационных финансовых технологий;
- обеспечение защиты прав потребителей финансовых услуг.

Основные направления включают описание предпосылок и основных тенденций в развитии информационной безопасности кредитно-финансовой сферы Российской Федерации, задачи и ключевые направления деятельности Банка России в области информационной безопасности и киберустойчивости. Для реализации поставленных задач в Банке России создан Департамент информационной безопасности, выполняющий в том числе функции Центра компетенций в области обеспечения информационной безопасности финансовой сферы.

Таким образом, действующие технологии обеспечения безопасности банковской деятельности должны быть ориентированы на решение следующих задач в области информационной безопасности и киберустойчивости, а именно: обеспечение киберустойчивости; защита прав потребителей финансовых услуг через мониторинг показателей уровня финансовых потерь; содействие развитию инновационных финансовых технологий в части контроля показателей риска реализации информационных угроз и обеспечение необходимого уровня информационной безопасности.

ВЫВОДЫ

Подводя итог проведенному исследованию, стоит отметить, что на финансово-хозяйственную деятельность банков влияет множество опасностей и угроз, возникновение которых должно быть спрогнозировано службой безопасности и приняты соответствующие меры по их предупреждению, ликвидации или минимизации. Рассмотрев всю совокупность способов минимизации рисков безопасности в коммерческом банке, можно сделать вывод о том, что существует высокая вероятность предотвращения угроз, влияющих на безопасность банковской системы. Всё зависит от применяемых способов снижения риска, на сколько эффективны они будут в той или иной ситуации.

Банк должен осуществлять регулярный мониторинг угроз безопасности, последовательно обеспечивая идентификацию банка, являющегося объектом мониторинга; формирование системы показателей оценки безопасности банка с учетом специфики его функционирования; сбор и подготовку информации, характеризующей состояние безопасности банка; выявление факторов, характеризующих перспективные направления развития банка; моделирование и формирование сценариев или стратегий развития банка; разработку предложений по предупреждению и нейтрализации угроз безопасности банка, что в конечном итоге будет способствовать совершенствованию и внедрению перспективных технологий обеспечения безопасности банковской деятельности.

СПИСОК ЛИТЕРАТУРЫ

1. Гусев В.С. Экономика и организация безопасности банков / В.С. Гусев. - СПб.: Очарованный странник, 2017. – 387 с.

2. Дворядкин, Е.Б. Экономическая безопасность: учебное пособие / Е.Б. Дворядкина, Н.В. Новикова. – Екатеринбург: Изд-во Урал. гос. экон. ун-та, 2018. – 346 с.

3. Исаев А.П. Организация и управление экономической безопасностью банков: учебник / А.П. Исаев. – СПб: ИПЦ СЗИУ - фил. РАНХиГС, 2016. – 332 с.

4. Овчинников В.Н., Сторожук, И.Н. Управление экономической безопасностью в условиях финансового кризиса / В.Н. Овчинников, И.Н. Сторожук. – Ростов на Дону: Южный Федеральный университет, 2019. – 192 с.

5. Сергеева И.А. Комплексная система обеспечения экономической безопасности банков: учеб. пособие / И.А. Сергеева, А.Ю. Сергеев. – Пенза: Изд-во ПГУ, 2017. – 122 с.

Azimut of Scientific Research: Economics and Administration.
2021. T.10. №3(36) *p-ISSN: 2309-1762; e-ISSN: 2712-8482*

6. Глазьев С.Ю. О неотложных мерах по укреплению экономической безопасности России и выводу российской экономики на траекторию опережающего развития. / С.Ю. Глазьев. – М.: Институт экономических стратегий, 2019. – 60 с.

7. Сараджева О.В. Вызовы банковской отрасли с позиции экономической безопасности / О. В. Сараджева, М.А. Ковтун. – М.: Флинта, 2019. – 385 с.

8. Волкова М.Н. Функциональные направления службы безопасности банка / М.Н. Волкова, Д.С. Иванников // Социально-экономические науки и гуманитарные исследования. - 2019. - № 4. - С. 144-147.

9. Донецкова О.Ю., Садыкова Л.М., Коробейникова Е.В. Влияние кризисов на деятельность финансовых посредников в России // Экономика. Налоги. Право. – 2021. – Т.14. - № 1. – С. 61-71.

10. Грабарчук О.В. Развитие финансовых технологий в банковской деятельности. Роль ЦБ / О.В. Грабарчук. – М.: Флинта, 2020. – 365 с.

11. Горбачев Д.В. Комплексный подход к организации деятельности службы экономической безопасности банка / Д.В. Горбачев, М.В. Кононова // Интеллект. Инновации. Инвестиции. - 2017. - № 1. - С. 165-170.

12. Банк России. Статистика национальной платежной системы за 2008-2020 гг. [Электронный ресурс]. Режим доступа: https://old.cbr.ru/statistics/psrf/

13. Домашова Д.В., Самошина Е.О. Формирование оптимальной стратегии системы обеспечения экономической безопасности / Д.В. Домашова, Е.О. Самошина // Безопасность информационных технологий. – 2018. – №4. – С. 93–96.

14. Банк России. Основные направления развития информационной безопасности кредитно-финансовой сферы на период 2019-2021 годов. [Электронный ресурс]. Режим доступа: https://cbr.ru/Content/Document/File/83253/onrib_2021.pdf

Статья поступила в редакцию 17.05.2021
Статья принята к публикации 27.08.2021