ISSN 1993-047X (Print) / ISSN 2410-0390 (Online)

УДК 001.895:004:336.7
JEL: E5, G21, L86, O3

DOI: http://dx.doi.org/10.21202/1993-047X.13.2019.3.1330-1342

Е. С. БОРИСОВА[1],
А. Л. БЕЛОУСОВ[1]

[1] *Финансовый университет при Правительстве Российской Федерации, г. Москва, Россия*

ИННОВАЦИИ КАК ИНСТРУМЕНТ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ДЕЯТЕЛЬНОСТИ БАНКОВСКОЙ СИСТЕМЫ

Контактное лицо:
Борисова Екатерина Сергеевна, аспирант, Финансовый университет при Правительстве Российской Федерации
Адрес: г. Москва, Ленинградский просп., 49, тел.: +7 (499) 943-98-55
E-mail: Borisova98@mail.ru
SPIN-код: 3521-0744
ORCID: http://orcid.org/0000-0001-5488-6474
Web of Science Researcher: http://www.researcherid.com/rid/ D-5589-2019

Белоусов Андрей Леонидович, доцент, кандидат экономических наук, Финансовый университет при Правительстве Российской Федерации
Адрес: г. Москва, Ленинградский просп., 49, тел.: +7 (499) 943-98-55
E-mail: ALBelousov@fa.ru
ORCID: http://orcid.org/0000-0002-9069-8830
Web of Science Researcher: http://www.researcherid.com/rid/L-2766-2018

Цель: рассмотрение инновационных технологий как способа защиты важной информации. Выявление взаимосвязи между информационной безопасностью и повышением результативности деятельности банков.
Методы: в процессе исследования проблемы противодействия банков кибератакам использовались системный подход, метод статистического анализа.
Результаты: проблема хищения, модификации, подделки информации приобрела наибольшее значение при развитии информационно-коммуникационных технологий. Кибератаки не только грозят потерей персональных данных, но и могут повлиять как на функционирование финансовых и коммерческих организаций, так и на экономику государства в целом. В данной статье киберугрозы рассматриваются в качестве приоритетной проблемы банков в условиях повсеместной цифровизации. Определены основные тенденции в области киберрисков, изучена динамика кибератак. Рассмотрены мероприятия, проводимые в России с целью предотвращения киберпреступлений. Систематизированы основные причины реализации киберугроз в банковской сфере, в числе которых не последнее место занимает человеческий фактор.
Сформулированы выводы о том, что для предотвращения киберугроз необходимо внедрение банковских инноваций, основанных в том числе на использовании позитивного зарубежного опыта по применению процессно ориентированного подхода, технологий BigData, блокчейн, биометрической идентификации клиентов.
Научная новизна: разработан комплекс мероприятий, направленных на внедрение банковских инноваций и снижение киберугроз, включая развитие киберстрахования.
Практическая значимость: предложенные рекомендации могут быть использованы в практической деятельности государственных органов и специалистов банковской сферы при принятии решений в области обеспечения кибербезопасности.

Ключевые слова: аспекты цифровой экономики; информационная безопасность; инновации; киберугрозы; BigData; блокчейн

Конфликт интересов: авторами не заявлен.

ISSN 1993-047X (Print) / ISSN 2410-0390 (Online)

Как цитировать статью: Борисова Е. С., Белоусов А. Л. Инновации как инструмент обеспечения информационной безопасности и повышения эффективности деятельности банковской системы // Актуальные проблемы экономики и права. 2019. Т. 13, № 3. С. 1330–1342. DOI: http://dx.doi.org/10.21202/1993-047X.13.2019.3.1330-1342

E. S. BORISOVA[1],
A. L. BELOUSOV[1]

[1] *Financial University under the Government of the Russian Federation, Moscow, Russia*

INNOVATIONS AS A TOOL FOR PROVIDING CYBER SECURITY AND INCREASING THE EFFICIENCY OF BANKING SYSTEM

Ekaterina S. Borisova, post-graduate student,
Financial University under the Government of the Russian Federation
Address: 49 Leningradskiy prospect, Moscow, tel.: +7 (499) 943-98-55
E-mail: Borisova98@mail.ru
SPIN-код: 3521-0744
ORCID: http://orcid.org/0000-0001-5488-6474
Web of Science Researcher: http://www.researcherid.com/rid/ D-5589-2019
Andrey L. Belousov, Associate Professor, PhD (Economics),
Financial University under the Government of the Russian Federation
Address: 49 Leningradskiy prospect, Moscow, tel.: +7 (499) 943-98-55
E-mail: ALBelousov@fa.ru
ORCID: http://orcid.org/0000-0002-9069-8830
Web of Science Researcher: http://www.researcherid.com/rid/L-2766-2018

Objective: to research innovative technologies as a means of protecting important information; to reveal the relationship between information security and improving the performance of banks.
Methods: the problem of banks' counteraction to cyberattacks was researched with systematic approach and a method of statistical analysis.
Results: under the development of information and communication technologies, the problem of theft, modification, and forgery of information has acquired the greatest importance. Cyberattacks threaten the loss of personal data and can affect both the functioning of financial and commercial organizations, and the economy of the state as a whole. In this article, cyber threats are viewed as a priority problem of banks under widespread digitalization. The main trends in the field of cyber risks are identified; the dynamics of cyber attacks is studied. The activities carried out in Russia to prevent cybercrime are considered. The main reasons for cyber threats in the banking sector are systematized, including the human factor.
Conclusions are made that in order to prevent cyberthreats it is necessary to introduce banking innovations based, among other things, on the positive foreign experience of applying the process-oriented approach, BigData technologies, blockchain, and biometric identification of customers.
Scientific novelty: a set of measures was developed to introduce banking innovations and reduce cyber threats, including the development of cyber insurance.
Practical significance: the proposed recommendations can be used in the practical activities of government agencies and banking professionals when making decisions in the field of cybersecurity.

Keywords: Aspects of digital economy; Information security; Innovations; Cyber threats; BigData; Blockchain

Conflict of Interest: No conflict of interest is declared by the authors.

For citation: Borisova E. S., Belousov A. L. Innovations as a tool for providing cyber security and increasing the efficiency of banking system, *Actual Problems of Economics and Law*, 2019, Vol. 13, No. 3, pp. 1330–1342 (in Russ.). DOI: http://dx.doi.org/10.21202/1993-047X.13.2019.3.1330-1342

ISSN 1993-047X (Print) / ISSN 2410-0390 (Online)

Введение

В XXI в. информация стала наиболее значительным ресурсом, используемым обществом во всех сферах жизнедеятельности. Все отрасли экономики подверглись информатизации и внедрению информационно-коммуникационных технологий (далее – ИКТ) как необходимому условию соответствия требованиям рынка и спросу потребителя [1]. Кроме того, производственная потребность в новейших информационных технологиях обусловлена тем, что компьютерная система может выполнять поставленные перед ней задачи гораздо быстрее, чем человек, и это экономит временные, финансовые и трудовые ресурсы. Также автоматизированный механизм может хранить большой объем информации, в кратчайшие сроки собирать, анализировать и распространять данные, минимизируя допущение ошибочных действий при выполнении той или иной операции.

В сегодняшних реалиях как никогда актуальна фраза немецкого бизнесмена Н. Ротшильда «Кто владеет информацией, тот владеет миром» [2]. Следовательно, важно не только уметь хранить информационные данные, но и защищать их от возможной утечки. С расширением возможностей персональных компьютеров, появлением Интернета и постоянным развитием технологий вопрос относительно усиления информационной безопасности с каждым днем становится все актуальнее с точки зрения первостепенной стратегической задачи как для современного общества, так и для любого государства [3]. Таким образом, под информационной безопасностью следует понимать систему защиты данных, которая позволяет определять уязвимые места и предупреждать о возможных рисках и сбоях в программной структуре хранения данных, информировать о действующей опасности, обеспечить конфиденциальность, ликвидировать или минимизировать внешние и внутренние угрозы несанкционированного доступа, способные повлиять на стабильность процесса документооборота и обмена данными в системе, а также привести к хищению, модификации и уничтожению информации [4].

Можно отметить следующие тенденции угроз в области информационной безопасности:

– рост кибератак, а также появление проблемы кибертерроризма, когда взлом секретных данных может привести к разрушению инфраструктуры страны [5–7];

– совершенствование методов взломов системы, которое происходит параллельно с развитием передовых технологий [8, 9];

– вредоносное воздействие на все цифровые платформы и электронные устройства [10, 11];

– появление новых вирусных систем [12].

С каждым годом растет количество попыток несанкционированного доступа к закрытым базам данных, а адреса кибератак увеличиваются на 40 % [13]. По данным Национального координационного центра по компьютерным инцидентам, в России было зафиксировано более 4,3 млрд внешних угроз, направленных на критическую информационную инфраструктуру[1]. Кроме того, по данным Сбербанка, ежегодные убытки от кибератак в РФ составляют более 600 млрд рублей (0,64 % ВВП РФ), а ущерб мировой экономики составляет 1 трлн долларов США[2].

По статистике, опубликованной японской компанией по разработке программного обеспечения для кибербезопасности Trend Micro, за 2018 г. в мире было в целом предотвращено 41 млрд случаев фишинга (интернет-мошенничества с целью получения пароля и логина для доступа к конфиденциальной информации). Также за год было совершено около 22 млн спам-атак и более 12 тысяч компрометаций деловой электронной переписки[3]. К сферам, наиболее подверженным кибератакам, относятся государственное и муниципальное управление, оборонные и военные структуры, банковские и финансовые институты [14]. Сфокусируем рассмотрение проблемы информационной безопасности непосредственно в рамках функционирования банковской системы, потому что получение доступа к многочисленным счетам клиентов банка является постоянным интересом со стороны киберпреступников.

---

[1] За год на Россию было совершено более четырех миллиардов кибератак. URL: https://rg.ru/2018/12/12/za-god-na-rossiiu-bylo-soversheno-bolee-chetyreh-milliardov-kiberatak.html (дата обращения: 17.02.2019).

[2] Кибератаки на банки: тренды, уязвимости и роль регулятора. URL: https://www.plusworld.ru/professionals/kiberataki-na-banki-trendy-uyazvimosti-i-rol-regulyatora/ (дата обращения: 18.02.2019).

[3] Статистика по киберугрозам в мире за 2018 г. URL: https://www.itbestsellers.ru/companies-analytics/detail.php?ID=41543 (дата обращения: 17.02.2019).

ISSN 1993-047X (Print) / ISSN 2410-0390 (Online)

Несмотря на то, что процесс компьютеризации банковской деятельности позволил повысить производительность труда сотрудников банка, а также внедрить новые финансовые продукты и технологии, появились сопутствующие риски, связанные с автоматизированными системами обработки информации. На современном этапе развития информационных технологий каждый банк заинтересован в разработке стратегии информационной безопасности, мероприятия которой способствовали бы снижению вероятности рисков, минимизации негативного эффекта в случаях успешных кибератак. Эффективная система защиты, внедренная в банковскую инфраструктуру, необходима для гарантии безопасного оказания клиентам банковских услуг, что не только укрепит уверенность граждан в сохранности своих данных, но и расширит клиентскую базу за счет стабильности и положительных отзывов [15].

Деловые партнеры, сотрудники, текущие и потенциальные клиенты заинтересованы в защите своих персональных данных при взаимодействии с информационной системой банка. Эффективность внутренней сети, ее стабильность и надежность являются стратегически важными вопросами любого банка, так как данная система должна не только не поддаваться вирусным атакам, но и уметь отслеживать источник угрозы и предотвращать дальнейшие кибернападения. Также от степени обеспечения безопасности автоматизированных информационных систем во многом зависят конкурентоспособность и репутация банка [16].

В рамках данной статьи поставлена задача рассмотреть современные инновационные технологии, ориентированные на обеспечение защиты конфиденциальной информации. В ходе исследования представляется важным выявить взаимосвязь между информационной безопасностью и повышением результативности деятельности банков, определить основные причины потери данных и факторы, влияющие на рост риска потенциальной киберугрозы, а также изучить положительный зарубежный опыт в сфере противодействия кибератакам в банковской системе.

Результаты исследования

Проблема поддержания и усиления информационной безопасности банковских систем нашла отражение в следующих нормативных правовых актах: Указ Президента РФ № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» от 22.12.2017, Федеральный закон № 161-ФЗ «О национальной платежной системе» от 27.06.2011[4], стандарты информационной безопасности организаций банковской системы России, установленные Центральным банком РФ (далее – ЦБ), направление «Информационная безопасность» в рамках реализации программы «Цифровая экономика Российской Федерации», утвержденной Распоряжением Правительства РФ № 1632-р от 28.07.2017 и т. д. [17].

Также стоит отметить, что в 2017 г. с участием Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак в качестве профилактических мероприятий проверки информационной безопасности было отработано более 300 серьезных возможных компьютерных инцидентов[5]. В этом же году все российские банки подключились к автоматизированной системе обработки инцидентов в сфере информационной безопасности, созданной Центром мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере. Это свидетельствует о заинтересованности органов власти в создании стабильной системы защиты банковских процессов на территории страны [18].

Наряду с такими причинами неуклонения от информационных угроз, как некачественное управление учетными записями и паролями, уязвимость программного обеспечения, устаревшие вирусные программы, недостаточная сетевая безопасность, можно отметить и человеческий фактор [19]. Это означает, что одним из наиболее решающих факторов при реализации политики банка относительно информационной безопасности является проблема некомпетентного или неаккуратного персонала. Так, служащие банка зачастую сами неосознанно наносят

[4] О национальной платежной системе: Федеральный закон № 161-ФЗ от 27.06.2011 (последняя редакция). URL: http://www.consultant.ru/document/cons_doc_LAW_115625/ (дата обращения: 22.02.2019).

[5] Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак. URL: http://www.tadviser.ru/index.php/Статья:Государственная_система_обнаружения,_предупреждения_и_ликвидации_последствий_компьютерных_атак_(ГосСОПКА) (дата обращения: 23.02.2019).

ISSN 1993-047X (Print) / ISSN 2410-0390 (Online)

ущерб банковской структуре, открывая сообщение от неизвестного отправителя с рабочей системы, которое в результате оказывается фишинговым письмом [20]. Ярким примером последствий данных действий можно считать инцидент, произошедший 4 июля 2018 г., когда злоумышленники получили таким способом доступ к автоматизированному рабочему месту клиента Центрального банка и вывели с корреспондентского счета более 58 млн рублей[6]. Также возможны случаи, когда служащие, наоборот, игнорируют подозрительную рассылку и не сообщают об этом руководству.

Важно отметить, что банковская деятельность во многом связана с безналичными системами международных банковских переводов, платежными системами Visa и Mastercard, а также использованием зарубежных облачных сервисов и т. д. Это означает, что множество различных коммерческих и производственных тайн в принципе находятся в открытом доступе для иностранных разработчиков данных информационных систем, что также может стать причиной хищения важной информации [21[7]].

Стоит отметить и такую неблагоприятную особенность российских банковских организаций, как несвоевременное проведение профилактических мероприятий, направленных на предотвращение кибератак [22]. Так, Сбербанк активизировал работы в области совершенствования системы информационной безопасности, приняв в 2015 г. концепцию кибербезопасности, только после ряда попыток взлома базы данных[8].

Сегодня в сфере виртуальных преступлений можно выявить две происходящие тенденции:

– на данный момент внимание хакеров в большей степени уделяется карточному процессингу (процесс обработки платежей по дебетовым и кредитным картам, интегрированных в платежные системы), чем интернет-банкингу (технология дистанционного доступа к банковским услугам посредством любого устройства, имеющего возможность подключения к Интернету);

– увеличение действий цифровых злоумышленников криптоиндустрии (ICO, кошельки, биржи, фонды)[9]. По данным компании по расследованию киберпреступлений Chainalysis, хакерам удалось украсть 10 % всех средств, инвестированных в ICO-проекты в 2017 г. В результате общий ущерб составил почти $225 млн, т. е. 30 000 инвесторов лишились в среднем по $7500 [23][10].

Также в 2017 г. началось распространение такой хакерской атаки, как джекпоттинг, под которой подразумевается повреждение системы безопасности банкоматов [25, 26].

В сегодняшних реалиях задачи предотвращения развития негативных тенденций по отношению к бесперебойному функционированию банка, а также сведение к минимуму причин возникновения угроз кибератак возложены на современные технологии. Банковские инновации представляют собой целесообразные нововведения, внедряемые в любую сферу деятельности банка для достижения положительного экономического и стратегического эффекта [27]. При этом должны удовлетворяться потребности клиентов и модернизироваться действующий процесс предоставления банковских услуг. Инновации рассматриваются не только как способ повышения показателей эффективности работы финансово-кредитной организации, но и в условиях постоянных рисков как инструмент обеспечения информационной безопасности. На данный момент нововведения в банковской сфере связаны с дистанционным обслуживанием клиентов, интернет-банкингом, электронными деньгами и т. д. [28]. Востребованный банк XXI в. – это банк с набором уникальных технологий, которые позволяют совершать финансовые операции в любом месте и в любое время быстро, эффективно и безопасно [29].

---

[6] Хакеры вывели 58 млн рублей со счета в Центробанке России. URL: https://www.novayagazeta.ru/news/2018/07/06/143104-hakery-vyveli-58-millionov-rubley-s-korrespondentskogo-scheta-v-tsentrobanke-rossii (дата обращения: 22.02.2019).

[7] Пример, утечка данных по программе лояльности Mastercard. URL: https://www.rbc.ru/finances/23/08/2019/5d602 2d59a79473df8a2c291 (дата обращения: 29.08.2019).

[8] Информационная безопасность банковской сферы в Российской Федерации. URL: https://nauchforum.ru/archive/ MNF_social/9(49).pdf (дата обращения: 18.02.2019).

[9] Восемь главных трендов в сфере киберпреступлений. URL: https://www.rspectr.com/articles/375/8-glavnyh-trendov-v-sfere-kiberprestuplenij (дата обращения: 18.02.2019).

[10] Итоги 2017 года. URL: https://www.group-ib.ru/blog/ report2017 (дата обращения: 18.02.2019). Более ранние примеры хакерских атак на ICO-проекты: [24].

ISSN 1993-047X (Print) / ISSN 2410-0390 (Online)

Кроме того, внедряемые в рабочий процесс инновации призваны обеспечивать следующие клиентоориентированные направления:

– простой, быстрый, круглосуточный и доступный всем поиск информации о продуктах и услугах банка с любого цифрового устройства;

– информационная безопасность данных пользователя;

– оперативная обратная связь;

– оптимизация бизнес-процессов [30].

Таким образом, сегодня происходит процесс реорганизации деятельности банков вокруг клиента посредством развития и внедрения технологии будущего, а также за счет стимулирования поведения, ориентированного на инновационную трансформацию [31]. Определяя эффект от внедрения инноваций банками в качестве выгодных решений, следует учитывать такие показатели функционирования банков, как рентабельность и рост активов, увеличение клиентских ресурсов, процентных доходов, а также ссуд и задолженностей клиентов [32].

Стратегически важно опираться на зарубежный опыт инновационного развития банковской системы, вести постоянный мониторинг появления на рынке ИКТ передовых технологий и качественно адаптировать их в отечественных условиях функционирования банков. Например, существует целый ряд инноваций IT-защиты, направленных на обеспечение безопасности персональных данных, предотвращение утечки информации, хранение и резервное копирование данных, защиту от кибератак, вирусов и других угроз взлома системы. В основе таких инноваций задействован процессно ориентированный подход (например, Service-oriented architecture, Cloud Computing, DataLeakPrevention и др.).

Наибольшее применение среди банков зарубежных стран находит технология BigData (или «Большие данные»), которая позволяет не только хранить несоизмеримый объем информации, оперативно находить нужные данные в больших массивах, обрабатывать и структурировать их, но и защищать информационные ресурсы от хищения, утраты, уничтожения, разглашения и искажения со стороны несанкционированных пользователей. С помощью больших данных можно гораздо эффективнее контролировать текущие проекты, быстро создавать новые и получать объективную оценку удовлетворенности всех пользователей. BigData в своей деятельности активно используют Mastercard, VISA, Facebook, Google и т. д. Например, американская компания IBM, занимающаяся аппаратным и программным обеспечением, а также консалтинговыми услугами в области IT-сервиса, применяет методы больших данных к проводимым денежным транзакциям. С их помощью было выявлено на 15 % больше мошеннических транзакций, что позволило увеличить сумму защищенных средств на 60 %. Внедрение данной технологии оказывает положительный эффект на рост качества клиентского сервиса, так как ускоряет взаимодействие с клиентами, повышает эффективность обработки запросов. Кроме того, происходят оптимизация планирования производства и снижение издержек на сервисные услуги. Так, один из крупнейших финансовых конгломератов в мире – HSBC – для решения проблемы мошенничества с кредитными картами внедрил систему BigData, вследствие чего эффективность службы по выявлению случаев мошенничества повысилась в три раза, а точность его выявления – в десять раз. За первые две недели применения данной инновации были выявлены криминальные схемы с общим потенциальным ущербом более 10 млн долларов. Также, по данным консалтинговой компании McKinsey, 76 % американских банков используют BigData для привлечения клиентов, построения лучшего взаимодействия и поддержки политики лояльности.

Однако эта инновация получила свое широкое распространение как среди обычных пользователей, органов власти и коммерческих организаций, так и среди злоумышленников. Например, по словам директора Департамента противодействия недобросовестным практикам Банка России, ЦБ ведет активный анализ сетей больших данных для выявления новых мошеннических схем и точек их распространения[11].

Одной из наиболее используемых организационно-экономических инноваций также можно считать технологию блокчейн, позволяющую хранить информацию в свободном доступе для всех заинтересованных лиц, которые не могут управлять или изменять ранее внесенные данные. Технология блокчейн успешно применяется в зарубежной практике управления активами и финансами коммерческих банков, организации систе-

[11] ЦБ использует BigData в борьбе с мошенниками. URL: http://stoppiramida.ru/news/1464/ (дата обращения: 19.02.2019).

ISSN 1993-047X (Print) / ISSN 2410-0390 (Online)

мы международных расчетов, что позволило снизить издержки и обеспечить безопасность использования интернет-технологий [33]. Каждое финансовое решение (приобретение акций, перевод денег и т. д.) записывается, образуя хронологическую «информационную цепочку». Это позволяет оценить законность действий банка и клиентов. Блокчейн уже практикуется такими банками, как CreditSuisse, GoldmanSachs, JP Morgan, Barclays. Кроме того, для развития данной инновации, а также для распространения блокчейна в финансовой торговле компания Microsoft объединилась с Bank of America MerrillLynch [34]. Также на базе блокчейн можно создавать любые открытые реестры, где будут фиксироваться сделки, а верификация платежей будет обеспечиваться средствами самой системы[12].

На данный момент в качестве способа противодействия несанкционированному доступу к охраняемым сведениям востребована биометрическая идентификация. В российских банках подобная инновационная технология постепенно внедряется и совершенствуется надежность данного способа взаимодействия с клиентом. Так, в «Альфа-Банке», в некоторых отделениях Сбербанка, «Промсвязьбанке» предоставляется опция идентифицирования клиента по отпечатку пальца. В «Тинькофф Банке», кроме отпечатка, существует еще и распознание по голосу через звонок в call-центр, благодаря которой клиенту не надо диктовать свои паспортные данные или называть кодовое слово.

Следуя за зарубежными трендами в области информационной безопасности, в 2018 г. в России после внесения изменений в Федеральный закон № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»[13] по инициативе Банка России и Министерства цифрового развития, связи и массовых коммуникаций РФ ПАО «Ростелеком» была создана цифровая платформа для дистанционной биометрической идентификации как важного условия предоставления коммерческих и государственных услуг – единая биометрическая система (далее – ЕБС). ЕБС предоставила возможность гражданам открыть счет, взять кредит или внести вклад без личного присутствия в банке. При регистрации клиента в системе вся информация централизованно хранится в ЕБС, где шифруется по требованиям Федеральной службы безопасности и Федеральной службы по техническому и экспортному контролю, а также постоянно проверяется уровень защищенности данных центром по информационной безопасности (Security Operation Cente) [35]. Биометрические данные включают следующие сведения о клиенте: ФИО, дату и место рождения, паспортные данные, адрес места проживания, контактную информацию, страховой номер индивидуального лицевого счета застрахованного лица в системе обязательного пенсионного страхования, а также идентификационный номер налогоплательщика[14].

По словам разработчиков, на 10 млн использований возможна только одна ошибка в авторизации[15]. Данный показатель объясняется следующими принципами построения системы:

– одновременная обработка голоса и лица клиента банка;

– привлечение ведущих российских разработчиков в области биометрии для развития ЕБС и снижения вероятности взлома данной инновационной технологии;

– постоянное комбинирование различных методов детектирования, что позволяет оперативно определять фальсификацию данных;

– биометрические данные гражданина поступают в ЕБС по защищенному отечественными криптоалгоритмами каналу связи;

– против несанкционированного пользования ресурсами используются технологии машинного обучения, а также проводится детальный анализ информации о проведенных действиях и операциях.

На результативность системы не влияет изменение прически клиента, ношение аксессуаров (например, очков), появление бороды или усов. Однако биоме-

[12] Инновации в банковской сфере. URL: http://www.bseu.by:8080/bitstream/edoc/67558/1/A.I._Klimovich%2C_N.A._Smirnov.pdf (дата обращения: 18.02.2019).

[13] О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма: Федеральный закон № 115-ФЗ от 07.08.2001 (последняя редакция). URL: http://www.consultant.ru/document/cons_doc_LAW_32834/ (дата обращения: 21.02.2019).

[14] Тренды развития ИТ в страховании. URL: http://www.tadviser.ru/index.php/Статья:Тренды_развития_ИТ_в_страховании_(киберстрахование_и_телематические_данные) (дата обращения: 20.02.2019).

[15] Как работает Единая биометрическая система. URL: https://habr.com/ru/company/rostelecom/blog/424751/ (дата обращения: 20.02.2019).

ISSN 1993-047X (Print) / ISSN 2410-0390 (Online)

трические данные необходимо обновлять каждые три года или досрочно в случаях проведенной пластической операции или получения травмы лица. Планируется, что до конца 2019 г. в любом банке России появится возможность зарегистрироваться в единой биометрической системе. Так, стоит отметить, что на январь 2019 г. система удаленной идентификации действовала в 20 % отделений Сбербанка[16]. Одним из крупных поставщиков биометрической информации в ЕБС также является «Тинькофф Банк».

Таким образом, проанализированные инновации выполняют следующие функции в области обеспечения информационной безопасности:

– своевременное реагирование на попытки несанкционированного доступа к базам данных;

– ведение протокола записей всех операций по локальной сети;

– идентификация пользователей, ресурсов и персонала системы информационной безопасности сети, в том числе опознание и установление подлинности пользователя по вводимым учетным данным.

Внедрение инноваций в систему информационной защиты позволило снизить количество реализованных угроз и уменьшить ущерб, о чем свидетельствует статистика Центрального банка РФ. Так, в 2018 г. убыток банков составил 76,49 млн рублей, что в 14 раз меньше, чем ущерб 2017 г. (более 1 млрд 78 млн рублей), а количество успешных атак – 20 к 22 соответственно[17]. Данные показатели свидетельствуют о целесообразности разработок и применения новейших технологий, обеспечивающих минимизацию уязвимости банковской системы. Однако сумма потерянных средств все равно остается значительной, что обуславливает необходимость ведения дальнейших исследований, развития систем информационного контроля и своевременного применения нововведений, которые не только обеспечат защиту информации, но и повысят эффективность функционирования банков.

На данный момент все большее распространение получает рынок «умного страхования», или, другими словами, страхования от киберугроз. Начало данной тенденции было положено рядом крупных зарубежных банков (Credit Suisse, Deutsche Bank и Lloyds), которые признали страхование рисков информационной безопасности наиболее оптимальным решением покрытия расходов при нападении на банковскую IT-инфраструктуру [36]. Так, наиболее крупной суммой страхования на данный момент являются облигации швейцарского банка Credit Suisse в размере 219 млн долларов США. Что касается России, то в соответствии с программой «Цифровая экономика Российской Федерации» расходы федерального бюджета на популяризацию киберстрахования составят 200 млн рублей [37]. По данным американской компании по программному обеспечению VMware, в 2017 г. более 52 % российских банков увеличили расходы на развитие своей системы информационной безопасности, что связано с активизацией киберугроз и ростом внедрения вредоносных программ. Тем не менее страховая компания Mains Insurance Brokers & Consultants прогнозирует рост данной суммы до 1 млрд рублей к 2025 г. Конкретным примером российского киберстрахования является технология «АльфаCyber», созданная в 2018 г. компанией «АльфаСтрахование» для защиты от киберрисков и снижения финансовых и информационных потерь[18]. Можно предположить дальнейшее развитие отечественного рынка страхования от хакерской деятельности ростом инвестиций в данную сферу, чтобы обеспечить действенную систему компенсации утечки важных данных.

Выводы

В результате проведенного исследования обоснована необходимость совершенствования систем защиты информации в работе кредитных организаций. Выявлены основные тенденции развития киберугроз для кредитных организаций. Отмечена значимость разработки и внедрения инноваций в финансовом секторе. Исследованы современные технологические решения, включаемые в бизнес-процессы ведущими банками страны, целью которых является противодействие совершению преступлений в области информационной безопасности. Изучен зарубежный опыт

[16] Удаленная идентификация. URL: https://www.cbr.ru/fintech/remote_authentication/ (дата обращения: 20.02.2019).

[17] ЦБ назвал ущерб российских банков от кибератак в 2018 году. URL: https://www.rbc.ru/rbcfreenews/5bc881ea9a7947189fe00a9a (дата обращения: 17.02.2019).

[18] Единая биометрическая система (ЕБС). URL: http://www.tadviser.ru/index.php/Продукт:Единая_биометрическая_система_(ЕБС) (дата обращения: 20.02.2019).

ISSN 1993-047X (Print) / ISSN 2410-0390 (Online)

борьбы с киберугрозами для субъектов банковского сектора.

Обобщая полученную информацию, можно подчеркнуть следующие актуальные меры информационной защиты данных:

– на государственном уровне совершенствовать стандарты по информационной безопасности в финансовых и коммерческих организациях и вести контроль их исполнения;

– увеличить финансирование области развития IT-технологий, направленных на защиту базы данных;

– качественно адаптировать зарубежные эффективные технологии информационной безопасности, учитывая отличия российского банкинга от иностранного;

– применять инновационные подходы в борьбе с кибератаками;

– проводить профилактические работы с целью тестирования и экспертизы качества системы безопасности;

– анализировать тенденции развития потребностей клиентов, чтобы целесообразно применять те или иные инновации;

– кооперировать банки с цифровой экосистемой, включая венчурные фонды, предпринимателей, научно-исследовательские центры для разработки наиболее эффективных программ противодействия виртуальным вирусам;

– расширять возможности отечественной банковской системы для снижения зависимости от зарубежных банков;

– организовать для сотрудников курсы повышения квалификации в области использования ИКТ с целью снижения практических ошибок, способствующих деятельности киберзлоумышленников, а также, возможно, заключать договоры с университетами о создании целевых мест, чтобы в будущем гарантированно привлекать специалистов по информационной безопасности [37].

Следовательно, развитию банковских инноваций будет способствовать снижение препятствующих внутренних и внешних факторов (макроэкономических, нормативно-правовых, финансовых, кадровых, технологических) [38].

Таким образом, процесс становления повсеместной цифровизации обуславливает необходимость банков быстро адаптироваться к новым условиям, мировым тенденциям в рамках обострения конкуренции и кризисных явлений на финансовых рынках. А значит, политика внедрения банковских инноваций – это инструмент достижения стабильности функционирования, конкурентоспособности, устойчивого экономического роста банков, сокращения издержек, пресечение кибермошенничества, рационального распределения финансовых ресурсов и как итог – совершенствование национальной платежной системы государства. Кроме того, применение инновационных решений, операций, новейших технологий в банковском секторе способствует реализации более совершенных банковских продуктов, повышению качества услуг, предоставляемых банками, что впоследствии приводит к росту доходов [39]. Исходя из этого, можно сделать вывод, что применение инноваций можно рассматривать как современный фактор получения прибыли [40].

Учет инновационных способов борьбы с несанкционированными доступами к информационной системе банка, своевременная корректировка условий и ликвидация причин для появления тех или иных рисков в совокупности сократит шансы на банковский кризис, уменьшит материальный ущерб банков от кибератак, что положительно скажется на экономических показателях страны. Проблема кибербезопасности систем управления в современном мире является актуальной, так как касается безопасности не только технических средств и устройств, но и интересов общества [41].

Список литературы

1. Белоусов А. Л. Некоторые аспекты внедрения информационных технологий в финансовой сфере // Инновационное развитие экономики. Будущее России: материалы и доклады V Всероссийской (национальной) научно-практ. конференции. 2018. С. 7–12.

2. Комаров А. В., Борисова Е. С., Кузбенова Э. Р. Цифровые технологии как платформа развития экономики // Экономическая трансформация и инновационные технологии: сборник материалов I Международной научно-практ. конференции. 2018. С. 27–30.

ISSN 1993-047X (Print) / ISSN 2410-0390 (Online)

3. Сургуладзе В. Ш. Информационная политика Российской Федерации: доктрина информационной безопасности в системе целеполагающих документов государственного стратегического планирования // Власть. 2017. Т. 25, № 2. С. 75–77.

4. Kulik T., Larsen P. G. Towards formal verification of cyber security standards // Труды Института системного программирования РАН. 2018. Т. 30. № 4. С. 79–94.

5. Lewis J. A. Assessing the risks of cyber terrorism, cyber war and other cyber threats. Washington, DC: Center for Strategic & International Studies, 2002.

6. Helms R., Costanza S. E., Johnson N. Crouching tiger or phantom dragon? Examining the discourse on global cyber-terror // Security journal. 2012. Vol. 25. № 1. Pp. 57–75.

7. Jang-Jaccard J., Surya Nepal. A survey of emerging threats in cybersecurity // Journal of Computer and System Sciences. 2014. № 80.5. Pp. 973–993.

8. Shema M. Hacking web apps: detecting and preventing web application security problems. Newnes, 2012.

9. McClure S., Scambray J., Kurtz G., Kurtz. Hacking exposed: network security secrets and solutions. 2009.

10. Carlin, Domhnall et al. You Could Be Mine (d): The Rise of Cryptojacking // IEEE Security & Privacy. 2019.

11. Libicki M. C. Second acts in cyberspace // Journal of Cybersecurity. 2017. № 3.1. Pp. 29–35.

12. Бураева Л. А. Кибертерроризм как новая и наиболее опасная форма терроризма // Пробелы в российском законодательстве. 2017. № 3. С. 35–37.

13. Безкоровайный М. М., Татузов А. Л. Кибербезопасность – подходы к определению понятия // Вопросы кибербезопасности. 2014. № 1 (2). С. 22–27.

14. Абдуллаев В. Г. Защита от спама в интернет пространстве // Радиоэлектроника и информатика. 2014. № 2. С. 35–38.

15. Белоусов А. Л. Условия формирования инновационной инфраструктуры экономики // Инновационное развитие современных социально-экономических систем: материалы III Международной заочной научно-практ. конференции. Министерство образования и науки Российской Федерации; ФГБОУ ВО «Комсомольский-на-Амуре государственный технический университет»; ФАО ДальНИИ рынка при Министерстве регионального развития РФ. 2016. С. 160–163.

16. Гулько А. А., Антонян М. Г., Гордеева Ю. С. Информационная безопасность в системе безопасности банка // Вектор экономики. 2018. № 3 (21). С. 39–46.

17. Бегларян М. Е., Мамакаев Х. В. Кибератаки и законодательство РФ // Право и практика. 2017. № 2. С. 46–50.

18. Солодкая А. М. Роль Центрального банка Российской Федерации в развитии финансовых технологий в отечественной экономике // Экономика и бизнес: теория и практика. 2019. № 1. С. 228–234.

19. Ревенков П. В. Кибербезопасность в условиях электронного банкинга // Современные тенденции развития науки и технологий. 2015. № 2–6. С. 97–101.

20. Казыханов А. А., Байрушин Ф. Т. Фишинг, как проблема для специалистов отдела ИБ // Символ науки. 2016. № 10. С. 53–54.

21. Капустин Ф. А. Информационная безопасность и защита информации в современном обществе // Актуальные проблемы авиации и космонавтики. 2016. Т. 2. С. 738–740.

22. Бундин М. В. Система информации ограниченного доступа и конфиденциальность // Вестник Нижегородского университета им. Н. И. Лобачевского. 2015. № 1. С. 120–130.

23. Lazarenko A., Avdoshin S. Financial Risks of the Blockchain Industry: A Survey of Cyberattacks // Proceedings of the Future Technologies Conference. Springer, Cham, 2018.

24. Mehar Muhammad Izhar et al. Understanding a revolutionary and flawed grand experiment in blockchain: the DAO attack // Journal of Cases on Information Technology (JCIT). 2019. № 21.1. Pp. 19–32.

25. Ogata Hisao et al. An ATM security measure for smart card transactions to prevent unauthorized cash withdrawal // IEICE Transactions on Information and Systems. 2019. № 02.3. Pp. 559–567.

26. Hsieh Ming-Li, Shun-Yung Kevin Wang. Routine activities in a virtual space: A Taiwanese case of an ATM hacking spree. 2018.

27. Бодиенкова В. С., Кондюкова Е. С. Электронные инновации в банковской сфере // Экономика и бизнес: теория и практика. 2017. Т. 1. № 4. С. 41–48.

28. Гирлина М. А. Инновации в банковском маркетинге // Современные проблемы и перспективы развития банковского сектора России: материалы III Всероссийской научно-практ. конференции с международным участием. Министерство образования и науки РФ. 2018. С. 34–39.

29. Luchian I., Ciobanu L. Theoretical concepts on bank of future // Economie si Sociologie: Revista Teoretico-Stiintifica. 2013. № 3. Pp. 48–52.

30. Аксенов В. С., Обухов В. В. Электронный банкинг в системе банковских услуг // Экономический журнал. 2013. № 3 (31). С. 75–83.

ISSN 1993-047X (Print) / ISSN 2410-0390 (Online)

31. Медведская Т. К., Запорожцева Е. Н. Устойчивость банковского бизнеса: тенденции и сценарии развития коммерческих банков // Экономика и современный менеджмент: теория, методология, практика. Пенза: Наука и просвещение, 2018. С. 32–44.

32. Lyeonov S. V., Samusevych Y. V., Demkiv I. M. The measurement of influence of innovations' implementation on the results of activities of commercial banks // Науковий вісник Полісся. 2018. № 1–2 (13). С. 68–76.

33. Шайданов Т. Р. Повышение качества банковских услуг в условиях развития цифровой экономики // Иннов: электронный научный журнал. 2018. № 6 (39). URL: http://www.innov.ru/science/economy/povyshenie-kachestva-bankovskikh-us/ (дата обращения: 22.02.2019).

34. Оголихина С. Д. Оценка необходимости применения инноваций в банковской системе России // Скиф. Вопросы студенческой науки. 2017. № 14 (14). С. 59–66.

35. Махнева О. А. Биометрические системы контроля доступа. Преимущества распределенных систем и облачных решений. Стационарный биометрический комплекс в составе распределенной облачной системы // Наука, техника и образование. 2016. № 12 (30). С. 60–64.

36. Дмитриев И. В. Направления повышения доверия в банковском секторе и развития системы страхования банковских вкладов граждан в России // Вестник МГИМО – Университета. 2014. № 34 (1). С. 158–163.

37. Сырецкий Г. А. Сквозные цифровые технологии и прорывные технологии кибербезопасности в контексте системного инжиниринга // Интерэкспо Гео-Сибирь. 2018. № 7. С. 254–260.

38. Борисова Е. С. Модернизация образования как фактор развития человеческого капитала в условиях автоматизации рынка труда // Постулат. 2018. № 11 (37). С. 78.

39. Флигинских Т. Н., Тарасова Т. Ю. Факторы, определяющие развитие инноваций в виде новых банковских продуктов // Креативная экономика. 2016. Т. 10, № 10. С. 1157–1168.

40. Белоусов А. Л., Левчук Е. Ю. Диджитализация банковского сектора // Финансы и кредит. 2018. Т. 24, № 2 (770). С. 455–464.

41. Kartashov K. Cybersecurity of vessel and possible ways of its provision // Crimean marine science research and technology conference 2018: сборник научных трудов по материалам Первой региональной научно-практ. конференции студентов, аспирантов и молодых ученых. Севастополь: ФГАОУВО «Севастопольский государственный университет», 2018. С. 21–26.

42. Lihtsinder B., Ivanova L., Zakharov S. Increasing profitability of banking products at the expense of the implementation of probability assessment of clients // 2016 3rd International Scientific-Practical Conference Problems of Infocommunications Science and Technology, PIC S and T 2016 – Proceedings 3. 2016. Pp. 178–180.

References

1. Belousov A. L. Some aspects of introducing information technologies in financial sphere, *Innovative development of economy. Future of Russia,* materials and reports of the 5th All-Russia (national) scientific-practical conference, 2018, pp. 7–12 (in Russ.).

2. Komarov A. V., Borisova E. S., Kuzbenova E. R. Digital technologies as a platform for economy development, *Economic transformation and innovative technologies,* collection of works of the 1st International scientific-practical conference, 2018, pp. 27–30 (in Russ.).

3. Surguladze V. Sh. Informationpolicy of the Russian Federation: doctrine of cyber security in the system of target-setting documents of state strategic planning, *Vlast'*, 2017, Vol. 25, No. 2, pp. 75–77 (in Russ.).

4. Kulik T., Larsen P. G. Towards formal verification of cyber security standards, *Trudy Instituta sistemnogo programmirovaniya RAN*, 2018, Vol. 30, No. 4, pp. 79–94.

5. Lewis J. A. *Assessing the risks of cyber terrorism, cyber war and other cyber threats*, Washington, DC, Center for Strategic & International Studies, 2002.

6. Helms R., Costanza S. E., Johnson N. Crouching tiger or phantom dragon? Examining the discourse on global cyber-terror, *Security journal*, 2012, Vol. 25, No. 1, pp. 57–75.

7. Jang-Jaccard J., Surya Nepal. A survey of emerging threats in cybersecurity, *Journal of Computer and System Sciences,* 2014, No. 80.5, pp. 973–993.

8. Shema M. *Hacking web apps: detecting and preventing web application security problems*, Newnes, 2012.

9. McClure S., Scambray J., Kurtz G., Kurtz. *Hacking exposed: network security secrets and solutions*, 2009.

10. Carlin, Domhnall et al. You Could Be Mine (d): The Rise of Cryptojacking, *IEEE Security & Privacy,* 2019.

11. Libicki M. C. Second acts in cyberspace, *Journal of Cybersecurity,* 2017, No. 3.1, pp. 29–35.

12. Buraeva L. A. Cyber terrorism as a new and most dangerous form of terrorism, *Probely v rossiiskom zakonodatel'stve*, 2017, No. 3, pp. 35–37 (in Russ.).

ISSN 1993-047X (Print) / ISSN 2410-0390 (Online)

13. Bezkorovainyi M. M., Tatuzov A. L. Cyber security – approaches to defining the notion, *Voprosy kiberbezopasnosti*, 2014, No. 1 (2), pp. 22–27 (in Russ.).

14. Abdullaev V. G. Protection against spam in the internet space, *Radioelektronika i informatika*, 2014, No. 2, pp. 35–38 (in Russ.).

15. Belousov A. L. Conditions for forming innovative infrastructure of economy, *Innovative development of modern social-economic systems*, materials of the 3rd International scientific-practical conference by correspondence, Ministerstvo obrazovaniya i nauki Rossiiskoi Federatsii, FGBOU VO "Komsomol'skii-na-Amure gosudarstvennyi tekhnicheskii universitet", FAO Dal'NII rynka pri Ministerstve regional'nogo razvitiya RF, 2016, pp. 160–163 (in Russ.).

16. Gul'ko A. A., Antonyan M. G., Gordeeva Yu. S. Cyber security in the security system of a bank, *Vektor ekonomiki*, 2018, No. 3 (21), pp. 39–46 (in Russ.).

17. Beglaryan M. E., Mamakaev Kh. V. Cyber attacks and the Russian legislation, *Pravo i praktika*, 2017, No. 2, pp. 46–50 (in Russ.).

18. Solodkaya A. M. Role of the Central bank of the Russian Federation in developing financial technologies in the Russian economy, *Ekonomika i biznes: teoriya i praktika*, 2019, No. 1, pp. 228–234 (in Russ.).

19. Revenkov P. V. Cyber security in digital banking, *Sovremennye tendentsii razvitiya nauki i tekhnologii*, 2015, No. 2–6, pp. 97–101 (in Russ.).

20. Kazykhanov A. A., Bairushin F. T. Fishing as a problem for cybersecurity specialists, *Simvol nauki,* 2016, No. 10, pp. 53–54 (in Russ.).

21. Kapustin F. A. Cyber security and information protection in the modern society, *Aktual'nye problemy aviatsii i kosmonavtiki*, 2016, Vol. 2, pp. 738–740 (in Russ.).

22. Bundin M. V. System of limited access to information and confidentiality, *Vestnik Nizhegorodskogo universiteta im. N. I. Lobachevskogo*, 2015, No. 1, pp. 120–130 (in Russ.).

23. Lazarenko A., Avdoshin S. Financial Risks of the Blockchain Industry: A Survey of Cyberattacks, *Proceedings of the Future Technologies Conference*, Springer, Cham, 2018.

24. Mehar Muhammad Izhar et al. Understanding a revolutionary and flawed grand experiment in blockchain: the DAO attack, *Journal of Cases on Information Technology (JCIT)*, 2019, No. 21.1, pp. 19–32.

25. Ogata Hisao et al. An ATM security measure for smart card transactions to prevent unauthorized cash withdrawal, *IEICE Transactions on Information and Systems*, 2019, No. 02.3, pp. 559–567.

26. Hsieh Ming-Li, Shun-Yung Kevin Wang. *Routine activities in a virtual space: A Taiwanese case of an ATM hacking spree*, 2018.

27. Bodienkova V. S., Kondyukova E. S. Digital innovations in banking, *Ekonomika i biznes: teoriya i praktika*, 2017, Vol. 1, No. 4, pp. 41–48 (in Russ.).

28. Girlina M. A. Innovations in banking marketing, *Modern problems and prospects of the Russian banking sector development*, works of the 3rd All-Russia scientific-practical conference with international participation, Ministerstvo obrazovaniya i nauki RF, 2018, pp. 34–39 (in Russ.).

29. Luchian I., Ciobanu L. Theoretical concepts on bank of future, *Economie si Sociologie: Revista Teoretico-Stiintifica*, 2013, No. 3, pp. 48–52.

30. Aksenov V. S., Obukhov V. V. Digital banking in the system of banking services, *Ekonomicheskii zhurnal*, 2013, No. 3 (31), pp. 75–83 (in Russ.).

31. Medvedskaya T. K., Zaporozhtseva E. N. Stability of banking business: trends and scenarios of commercial banks development, *Ekonomika i sovremennyi menedzhment: teoriya, metodologiya, praktika*, Penza, Nauka i prosveshchenie, 2018, pp. 32–44 (in Russ.).

32. Lyeonov S. V., Samusevych Y. V., Demkiv I. M. The measurement of influence of innovations' implementation on the results of activities of commercial banks, *Naukovii visnik Polissya*, 2018, No. 1–2 (13), pp. 68–76.

33. Shaidanov T. R. Increasing the quality of banking services under digital economy development, *Innov: elektronnyi nauchnyi zhurnal*, 2018, No. 6 (39), available at: http://www.innov.ru/science/economy/povyshenie-kachestva-bankovskikh-us/ (access date: 22.02.2019) (in Russ.).

34. Ogolikhina S. D. Assessment of the need to apply innovations in the Russian banking system, *Skif. Voprosy studencheskoi nauki*, 2017, No. 14 (14), pp. 59–66 (in Russ.).

35. Makhneva O. A. Biometric systems for access control. Advantages of distributed systems and cloud solutions. Stationary biometric complex within a distributed cloud system, *Nauka, tekhnika i obrazovanie*, 2016, No. 12 (30), pp. 60–64 (in Russ.).

36. Dmitriev I. V. Directions of increasing trust in the banking sector and developing the system of insuring bank deposits of the Russian citizens, *Vestnik MGIMO – Universiteta*, 2014, No. 34 (1), pp. 158–163 (in Russ.).

ISSN 1993-047X (Print) / ISSN 2410-0390 (Online)

37. Syretskii G. A. End-to-end digital technologies and breakthrough cybersecurity technologies in the context of systemic engineering, *Interekspo Geo-Sibir'*, 2018, No. 7, pp. 254–260 (in Russ.).

38. Borisova E. S. Modernizing education as a factor of human capital development under automation of labor market, *Postulat*, 2018, No. 11 (37), p. 78 (in Russ.).

39. Fliginskikh T. N., Tarasova T. Yu. Factors determining innovations development in the form of new banking products, *Kreativnaya ekonomika*, 2016, Vol. 10, No. 10, pp. 1157–1168 (in Russ.).

40. Belousov A. L., Levchuk E. Yu. Digitalization of banking sector, *Finansy i kredit*, 2018, Vol. 24, No. 2 (770), pp. 455–464 (in Russ.).

41. Kartashov K. Cybersecurity of vessel and possible ways of its provision, *Crimean marine science research and technology conference 2018*, sbornik nauchnykh trudov po materialam Pervoi regional'noi nauchno-prakt. konferentsii studentov, aspirantov i molodykh uchenykh, Sevastopol', FGAOUVO "Sevastopol'skii gosudarstvennyi universitet", 2018, pp. 21–26.

42. Lihtsinder B., Ivanova L., Zakharov S. Increasing profitability of banking products at the expense of the implementation of probability assessment of clients, *2016 3rd International Scientific-Practical Conference Problems of Infocommunications Science and Technology, PIC S and T 2016 – Proceedings 3*, 2016, pp. 178–180.

Дата поступления / Received 28.06.2019
Дата принятия в печать / Accepted 02.09.2019
Дата онлайн-размещения / Available online 25.09.2019