УДК 336.276.23:658.15

ФИНАНСОВЫЕ МОШЕННИЧЕСТВА В БАНКОВСКОЙ СФЕРЕ

Шамрина Светлана Юрьевна[1], канд. экон. наук, доц.
Ломакина Анна Николаевна[2], канд. экон. наук, доц.
Фролов Александр Витальевич[1], канд. экон. наук, доц.

[1] Ставропольский государственный аграрный университет, Зоотехнический пер., 12, Ставрополь, Россия, 355017; e-mail: svetlana2202@list.ru; froloffman@mail.ru

[2] Невинномысский институт экономики, управления и права, ул. Зои Космодемьянской, 1, Невинномысск, Россия, 357101; email: annancfu@yandex.ru

Цель: систематизация, теоретическое обоснование подходов к формированию эффективной системы предупреждения финансового мошенничества в банковской сфере посредством глобальной сети интернет. Для достижения данной цели в статье рассмотрены виды, причины и условия появления и распространения интернет-мошенничества, а также способы его предотвращения. *Обсуждение*: в связи с активным ростом интернет-мошенничества в финансовой сфере вопросы о видах кибермахинаций, причинах, способах их выявления и методов защиты приобретают актуальность. Растущее число киберпреступлений в финансовом секторе свидетельствует о несовершенстве законодательства в данной сфере, финансовой безграмотности населения, что сказывается не только на благосостоянии населения, но и на финансовой системе в целом. Анализ ситуации, сложившейся в финансовой сфере России к настоящему времени, свидетельствует о синергии негативных воздействий всемирного экономического кризиса и многообразных внутренних причин. Учитывая российскую финансовую и хозяйственную специфику, уровень распространения и размеры ущерба от финансового мошенничества в самых разнообразных его формах и видах стали одними из важных критериев для оценки криминогенной обстановки в нашей стране. Глобализация мировой цивилизации сделала очевидной взаимозависимость мировой и российской финансовых систем. При этом осложняет ситуацию то, что в настоящее время характер мошенничества в нашей стране приобретет более изощренный интеллектуальный характер. Из вышесказанного возникает необходимость исследования проблемы, связанной с мошенническими действиями в рамках финансовых рынков в целях своевременного выявления мошенников и во избежание противоправных действий

с их стороны. *Результаты*: рассмотрены виды мошеннических действий и предложены решения по противодействию им. Представлен алгоритм действий, направленных на установление благонадежности компании. Результатом работы являются основные профилактические мероприятия, направленные на предупреждение и противодействие интернет-мошенничеству.

Ключевые слова: интернет-мошенничество, финансы, банки, киберпреступления, информационные технологии, защита.

DOI: 10.17308/meps.2021.5/2590

Введение

Согласно статистическим данным, Россия – одно из государств, в котором процветают и бурно развиваются разные виды мошенничества. Особенность российского законодательства заключается в отсутствии достаточного количества специальных норм по их противодействию.

Финансовое мошенничество занимает основополагающее место среди всех видов мошенничества. С активным развитием новых технологий финансовое мошенничество тоже не стоит на месте, адаптируется к современным условиям. На данный момент мошенничество обрело высокоинтеллектуальный характер. Мошенники применяют как и новые технологии, так и различные психологические методики.

Задачи исследования

Для обеспечения экономической безопасности банковской системы рассмотрим сущность и виды мошеннических действий в банковской сфере, совершаемые с помощью Всемирной паутины, и способы предотвращения незаконных финансовых операций, а также ответственность за совершение мошенничеств в России.

Методология исследования

В основе фундаментальных и прикладных исследованийя отечественных ученых и практиков – нормативно-правовые документы. Использовались следующие методы: наблюдение, логический анализ, синтез, индукция и дедукция.

Обсуждение результатов

В настоящее время в связи с развитием различных технологий, компьютерных сетей, компьютеризации всей экономики очень большое распространение получили финансовые мошенничества в сети интернет.

В настоящее время главную роль в развитии рыночных отношений играют кредитные организации. Так как в кредитных организациях большинство населения хранят свои сбережения, и именно эти организации могут проявлять свою роль в развитии экономики страны. Банки больше всего подвергаются появлению финансовых рисков и угроз, которые касаются и сотрудников банка, и клиентов [7]. Поэтому в банковской сфере важно обеспечить высокий уровень экономической безопасности [3].

Существует множество видов современных мошенничеств, ниже представлены некоторые из них:

Рис. 1. Виды финансовых мошенничеств

Экономическая безопасность банковской системы – это состояние эффективного использования финансовых ресурсов для предотвращения и обеспечения функционирования банковской деятельности. Основной целью является создание основы и перспектив развития банковской системы независимо от факторов угроз, а также достижение максимальной стабильности функционирования [10].

По данным лаборатории «Касперского», за 2018 год количество интернет-мошенничеств в банковских структурах составило примерно 3 тыс. атак с использованием методов социальной инженерии. А в первом квартале 2020 года количество интернет-атак выросло в три раза по сравнению с 2018 годом и составило около 10 тыс. При этом потенциальный ущерб, по данным лаборатории, может составлять до 3 млрд руб. за один квартал. В 2020 году в связи с угрозой коронавирусной инфекции мошенничество в сети интернет набирает мощные обороты, когда пользователям предлагают различные компенсации при оплате небольшой комиссии. Поэтому сегодня очень важно делать акцент на проверку любой информации из различных источников сети интернет, чтобы защититься и не стать жертвой мошенников [8].

Экономические преступления все чаще совершаются с помощью глобальной сети. Мошенники активно используют интернет для проникновения в различные базы данных, тем самым имеют воздействиея на различный круг лиц.

Мошенничество представляет собой преступление, совершаемое при злоупотреблении доверием. Мошенники и злоумышленники для обмана часто пользуются знаниями психологии и воздействуют на психику людей. Доверчивостью людей пользуются мошенники при совершении афер не только в реальном мире, но теперь уже и виртуальном.

Наиболее распространенные виды онлайн-мошенничества называются фишингом и спуфингом. Фишинг представляет собой процесс сбора личной информации через электронную почту или веб-сайты, утверждающие,

что они являются законными. Эта информация может включать имена пользователей, пароли, номера кредитных карт, номера социального страхования и т. д. Часто электронные письма направляют пользователя на веб-сайт, где нужно обновить свою личную информацию. Поскольку эти сайты часто выглядят «официальными», мошенники надеются, что обманом заставят раскрыть ценную информацию. Это часто приводит к краже личных данных и финансовым потерям [4].

Шпионское программное обеспечение (далее – ПО) и вирусы – это вредоносные программы, которые загружаются на компьютер без вашего ведома. Целью этих программ может быть сбор или уничтожение информации, нарушение производительности компьютера или перегрузка вас рекламой. Вирусы могут распространяться, заражая компьютеры, а затем размножаясь. Шпионское ПО маскируется под легитимное приложение и встраивается в компьютер, где затем отслеживает вашу активность и собирает информацию. Мошеннические «всплывающие окна» – это вид онлайн-мошенничества, часто используемый для получения личной информации. Это окна или объявления, которые внезапно появляются над или под окном, которое вы просматриваете в данный момент. Поддельные веб-сайты или всплывающие окна используются для сбора вашей личной информации.

В электронное письмо могут быть включены дополнительные ссылки на реальные веб-сайты, чтобы заставить пользователя поверить в то, что это письмо является законным.

Мошеннические веб-сайты, электронные письма или всплывающие окна могут запросить личную информацию (номер счета, номер социального страхования, дату рождения и т. д.).

Всплывающие окна часто возникают из-за установленных на компьютере программ, называемых «рекламным ПО» или «шпионским ПО».

Эти программы следят за просмотрами в интернет-сфере и при скачивании бесплатных файлов содержатся в них. Существуют различные программы по размещению рекламы на сайтах, некоторые такие программы могут содержать вирусы при нажатии на нее, тем самым данный вирус может не только нарушить работы вашего ПО, но и записывать и передавать всю личную информацию третьим лицам [1, 2].

Если сразу не принять нужные меры предосторожности, можно подвергнуть опасности себя, а именно свои счета и личную информацию.

1. Фишинг, спуфинг, мошенничество с всплывающими окнами – виды онлайн-мошенничества, используемые для получения личной информации.

Троянский конь – вирус, который может записывать ваши нажатия клавиш. Он может находиться во вложении или доступен по ссылке в электронном письме, на веб-сайте или во всплывающем окне. Поддельные веб-сайты – URL-адреса, которые перенаправляют вас на мошеннический сайт. Чтобы проверить URL-адрес, вы можете ввести или вырезать и вставить URL-адрес в новое окно веб-браузера, и если он не приведет вас на закон-

ный веб-сайт или вы получите сообщение об ошибке, это, вероятно, было просто прикрытием для мошеннического веб-сайта.

2. Активируйте блокировщик всплывающих окон. В интернете доступны бесплатные программы, локирующие всплывающие окна.

Обязательно выполните поиск виИнтернете по запросу «блокировщик всплывающих окон» или изучите варианты, предлагаемые основными поисковыми системами. Перед загрузкой вам необходимо подтвердить, что эти программы принадлежат законным компаниям. После того как вы установили блокировщик всплывающих окон, вы должны определить, блокирует ли он информацию, которую вам нужно просмотреть, или получить к ней доступ. В этом случае вам следует рассмотреть возможность отключения блокировщика, когда вы находитесь на веб-сайтах, которые, как вы знаете, используют всплывающие окна для предоставления информации, которая вам нужна или которую вы хотите просмотреть.

3. Регулярно проверяйте свой компьютер на наличие шпионского ПО.

Вы можете устранить потенциально опасные всплывающие окна, удалив все шпионское или рекламное ПО, установленное на вашем компьютере. Шпионское и рекламное ПО – это программы, которые отслеживают вашу активность в интернете и потенциально передают информацию в источник с сомнительной репутацией. Выполните поиск в интернете по запросу «шпионское ПО» или «рекламное ПО», чтобы найти бесплатные программы для удаления шпионского ПО. Как и в случае с блокировщиком всплывающих окон, вы должны быть уверены, что ваша программа удаления не блокирует и не удаляет требуемые элементы, и если это так, подумайте об отключении ее для некоторых веб-сайтов.

4. Избегайте загрузки программ из неизвестных источников. Загрузки могут содержать скрытые программы, которые могут поставить под угрозу безопасность вашего компьютера. Точно так же вложения электронной почты от неизвестных отправителей могут содержать вредоносные вирусы.

5. Поддерживайте актуальность операционной системы компьютера и интернет-браузера.

6. Необходимо регулярно обновлять антивирусные программные обеспечения. Антивирусные программы должны часто обновляться для защиты от новых вирусов. Выберите надежного поставщика. Загрузите обновления антивируса, как только вы получите уведомление о наличии поисковыми системами. Перед загрузкой вам необходимо подтвердить, что эти программы принадлежат законным компаниям. После того как вы установили блокировщик всплывающих окон, вы должны определить, блокирует ли он информацию, которую вам нужно просмотреть, или получить к ней доступ. В этом случае вам следует рассмотреть возможность отключения блокировщика, когда вы находитесь на веб-сайтах, которые, как вы знаете, используют всплывающие окна для предоставления информации, которая вам нужна или которую вы хотите просмотреть.

7. Держите свои пароли в секрете. Регулярно меняйте их, используя сочетание цифр и символов. Настоящие электронные средства защиты включают в себя понимание нашими клиентами фактов мошенничества, того, как они происходят, как они влияют на вас и какие инструменты и решения предлагает банк, чтобы помочь вам [11].

Мошенничество независимо от среды проявления уголовно наказуемо. Ответственность за совершение таких преступлений предусмотрено статьями 159 и 159.6 УК РФ. Наивысшим наказанием по данным статьям является 10 лет лишения свободы и штраф 1 млн рублей. Минимальным наказанием – штраф до 120 тыс. рублей. Также за данное преступление предусматривается административная ответственность статьей 7.27 КоАП РФ и предусматривает наказание – арест на 15 суток и штраф на сумму от 1 тыс. руб. [9, 6].

Под влиянием экономической глобализации и интеграции проводятся изменения в российском законодательстве, направленном на борьбу с мошенничеством, регулирующем в том числе и деятельность банков. Ускорение интеграционных процессов и создание единого экономического пространства невозможны без значительного расширения взаимодействия государств в финансовой сфере и формирования в перспективе всеобщего рынка финансовых и банковских услуг. Интеграция позволит достичь единства и целостности бизнес-процессов, связанных с удовлетворением интересов владельцев, государства и потребителей [5].

Все мошенничества в финансовой сфере объединяет одно: преступники без принуждения, с согласия самих людей получают их денежные средства. При этом потерпевшие думают, что передают эти деньги в обмен на какие-либо законные блага – недвижимое имущество, товары в интернет-магазинах, наследство. На самом же деле никаких «законных благ» нет, люди просто теряют свои деньги, не получая ничего взамен. Злоумышленники же изначально знают, что они не имеют никаких правовых оснований для получения экономического обогащения. Все банковские мошенничества можно предотвратить, если соблюдать некоторые требования.

Таблица 1

Ситуации и решения по противодействию мошенничеству

Ситуации	Решения
При краже карты	Немедленно обратиться в банк, позвонить или посетить лично
При получении смс-сообщения о списании суммы с банковского счета или при поступлении запроса на подтверждение неизвестной операции	Позвонить в банк или посетить лично и уточнить данные об операции. Никому не разглашать данные банковской карты и пароли к доступу в личные кабинеты.
Использование банкомата для совершения операций	Внимательно осмотреть сам банкомат. Не передавать банковскую карту третьим лицам. Прикрывать клавиатуру при вводе ПИН-кода карты.

Окончание табл. 1

Ситуации	Решения
При получении различных электронных писем	Нельзя открывать подозрительные письма. При открытии подозрительных писем не переходите по ссылкам.
Производя поиск в сети интернет	Не посещать сайты, не вызывающие доверия. Не устанавливать подозрительные программы. Установить антивирусные программы.
При подозрительных звонках, например, с банков	Не раскрывать персональные данные звонящим с незнакомых номеров.

Для заключения сделок с различным компаниями по поводу вложения каких-либо финансовых средств обязательно нужно удостовериться в благонадежности компании.

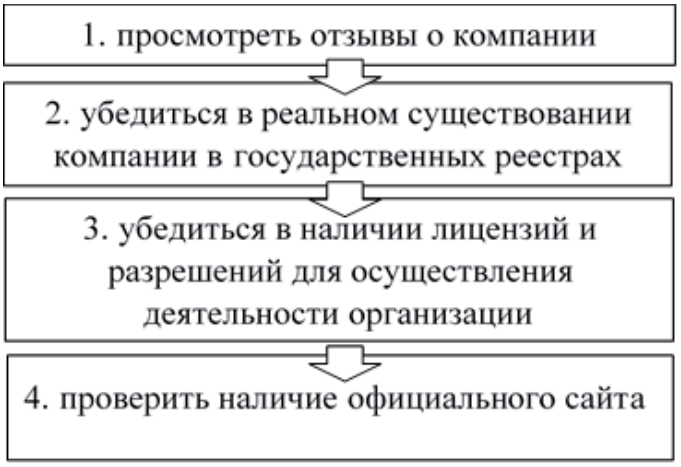

Рис. 2. Способы убеждения в благонадежности компаний

Финансовое мошенничество является довольно опасным и частным явлением, способным проявляться в различных его формах. И даже несмотря на то, что рассматриваемая проблема кажется от нас далекой, необходимо быть с ней знакомым. Она может коснуться любого из нас, каким бы осторожным человек ни был.

Заключение

Таким образом, современное экономическое развитие нашей страны тесно связано с глобальной системой мирового хозяйства, поэтому использование мирового опыта борьбы с финансовым мошенничеством с учетом специфики российских реалий дает возможность для создания эффективно действующих механизмов по профилактике и противодействию мошенничеству. Профилактическая направленность в борьбе с финансовым мошенничеством, заключающаяся в совершенствовании законодательства, повы-

шении финансовой грамотности населения, развитии процессов интеграции в сфере защиты персональной информации, может стать действенным инструментом борьбы с данным преступлением.

Список источников

1. Богданов А.В., Ильинский И.М., Хазов Е.Н. Киберпреступность и дистанционное мошенничество как одна из угроз современному обществу // *Криминологический журнал*, 2020, no. 1, с. 15-20.

2. Белоножко Е.С., Чеджемов Г.А. Мошенничество в сети интернет // *Наука XXI века: актуальные направления развития*. Самара, СГЭУ, 2017, no. 1-1, с. 86.

3. Васюкова В.А., Воробьева И.В., Ломакина А.Н. Стратегические траектории развития при защите интересов субъектов информационных отношений в сфере услуг // *Научный вестник Государственного автономного образовательного учреждения высшего профессионального образования «Невинномысский государственный гуманитарно-технический институт»*, 2018, no. 2, с. 94-97.

4. Гладкий А. *Мошенничество в интернете. Методы удаленного выманивания денег, и как не стать жертвой злоумышленников.* Москва, АВТОР, 2018.

5. Дементьева, А.Н. Интеграция как инструмент повышения эффективности предпринимательских структур // *Достижения науки и техники АПК*, 2006, no. 6, с. 55-56.

6. КоАП РФ. Доступно: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&ts=115974575053225977630935l7&cacheid=B7414D03067EA03CF1D49CD497FBBA21&mode=splus&base=LAW&n=204183&rnd=0.7348916463651269#1jfc94ldgrd (дата обращения: 12.03.2021).

7. Ломакина А.Н., Шамрина С.Ю., Манчук Е.П. Маркетинговые исследования рынка банковских платежных карт на примере ВТБ // *Финансы и кредит,* 2018, Т. 24, no. 6(774), с. 1403-1419.

8. Официальный сайт компании «Лаборатория Касперского». Доступно: http://www.kaspersky.ru (дата обращения: 22.03.2021).

9. Сотникова Л.Н., Ткачева М.В. Банковская система РФ: состояние и перспективы развития // *Вестник Воронежского государственного университета инженерных технологий*, 2015, no. 2 (64), с. 260-266.

10. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (ред. от 18 февраля 2020 г.) Доступно: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&ts=1579205278061807973679726 8&cacheid=6CBBAE03A4FCF60CB46203D978DCB328&mode=splus&base=LAW&n=325409&rnd=0.32122736858355916#4obabkd24ic (дата обращения: 12.03.2021).

11. Шамрина С.Ю., Ломакина А.Н. Сценарный анализ стресс-тестирования при оценке основных видов рисков кредитной организации // *Финансы и кредит*, 2018, Т. 24, no. 7(775), с. 1736-1750.

12. Шейнов В.П. *Как защититься от обмана и мошенничества*: монография. Москва, Харвест, 2019.

FINANCIAL FRAUD IN THE BANKING SPHERE

Shamrina Svetlana Yurievna[1], Cand. Sc. (Econ.), Assoc. Prof.
Lomakina Anna Nikolaevna[2], Cand. Sc. (Econ.), Assoc. Prof.
Frolov Alexander Vitalievich[1], Cand. Sc. (Econ.), Assoc. Prof.

[1] Stavropol State Agrarian University, Zootechnical per. 12, Stavropol, Russia, 355017; e-mail: svetlana2202@list.ru; froloffman@mail.ru

[2] Nevinnomyssk Institute of Economics, Management and Law, st. Zoya Kosmodemyanskaya, 1, Nevinnomyssk, Russia, 357101; e-mail: annancfu@yandex.ru

Purpose: systematization, theoretical substantiation of approaches to the formation of an effective system for the prevention of financial fraud in the banking sector through the global Internet. To achieve this, the article discusses the types, reasons and conditions for the emergence and spread of Internet fraud, as well as ways to prevent them. *Discussion*: in connection with the active growth of Internet fraud in the financial sector, questions about the types of cyber fraud, the reasons, how they are detected and methods of protection are becoming relevant. The growing number of cybercrimes in the financial sector testifies to the imperfection of legislation in this area, financial illiteracy of the population, which affects not only the welfare of the population, but also the financial system as a whole. An analysis of the situation that has developed in the financial sphere of Russia to date shows the synergy of the negative impacts of the global economic crisis and various internal causes. Taking into account the Russian financial and economic specifics, the level of distribution and the extent of damage from financial fraud in its most diverse forms and types have become one of the important criteria for assessing the crime situation in our country. The globalization of world civilization has made the interdependence of the world and Russian financial systems obvious. At the same time, the situation is complicated by the fact that at present the nature of fraud in our country will acquire a more sophisticated intellectual character. From the foregoing, it becomes necessary to investigate the problem of fraudulent activities in the financial markets in order to timely identify fraudsters and to avoid illegal actions on their part. *Results*: the types of fraudulent activities were considered and solutions were proposed to counteract them. An algorithm of actions aimed at establishing the reliability of the company is presented. The result of the work is the main preventive measures aimed at preventing and countering Internet fraud.

Keywords: internet, fraud, finance, banks, cybercrime, information technology, protection.

References

1. Bogdanov A.B., Il'inskij I.M., Hazov E.N. Kiberprestupnost' i distancionnoe moshennichestvo kak odna iz ugroz sovremennomu obshchestvu [Cybercrime and remote fraud as one of the threats to modern society]. *Kriminologicheskij zhurnal*, 2020, no. 1, pp. 15-20. (In Russ.)

2. Belonozhko E.S., CHedzhemov G.A. Moshennichestvo v seti Internet [Fraud in the Internet]. *Nauka XXI veka: aktual'nye napravleniya razvitiya*. Samara. SGEU, 2017, no. 1-1, pp. 86. (In Russ.)

3. Vasyukova V.A., Vorob'eva I.V., Lomakina A.N. Strategicheskie traektorii razvitiya pri zashchite interesov sub"ektov informacionnyh otnoshenij v sfere uslug [Strategic trajectories of development in the protection of the interests of subjects of information relations in the sphere of services]. *Nauchnyj vestnik Gosudarstvennogo avtonomnogo obrazovatel'nogo uchrezhdeniya vysshego professional'nogo obrazovaniya «Nevinnomysskij gosudarstvennyj gumanitarno-tekhnicheskij institut»*, 2018, no. 2, pp. 94-97. (In Russ.)

4. Gladkij A. *Moshennichestvo v Internete. Metody udalennogo vymanivaniya deneg, i kak ne stat' zhertvoj zloumyshlennikov* [Fraud on the Internet. Methods of remote money extortion, and how not to become a victim of intruders]. Moscow, AVTOR, 2018. (In Russ.)

5. Dement'eva A.N. Integraciya kak instrument povysheniya effektivnosti predprinimatel'skih struktur [Integration as a tool for improving the efficiency of business structures]. *Dostizheniya nauki i tekhniki APK*, 2006, no. 6, pp. 55-56. (In Russ.)

6. KoAP RF [Elektronnyj resurs]. [Administrative Code of the Russian Federation]. Available at: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&ts=1159745750532259776309351 7&cacheid=B7414D03067EA03CF1D49CD497FBBA21&mode=splus&base=LAW&n=204183&rnd=0.7348916463651269#1jfc94ldgrd (assessed: 12.03.2021). (In Russ.)

7. Lomakina A.N., SHamrina S.YU., Manchuk E.P. Marketingovye issledovaniya rynka bankovskih platezhnyh kart na primere VTB [Marketing research of the market of bank payment cards on the example of VTB]. *Finansy i kredit*, 2018, vol. 24, no. 6(774), pp. 1403-1419. (In Russ.)

8. Oficial'nyj sajt kompanii «Laboratoriya Kasperskogo». [Official website of Kaspersky Lab]. Available at: http://www.kaspersky.ru (assessed: 22.03.2021) (In Russ.)

9. Sotnikova L.N., Tkacheva M.V. Bankovskaya sistema RF: sostoyanie i perspektivy razvitiya [Banking system of the Russian Federation: state and prospects of development]. *Vestnik Voronezhskogo gosudarstvennogo universiteta inzhenernyh tekhnologij,* 2015, no. 2 (64), pp. 260-266. (In Russ.)

10. Ugolovnyj kodeks Rossijskoj Federacii ot 13 iyunya 1996 g. no. 63-F3 (red. ot 18 fevralya 2020 g.) [The Criminal Code of the Russian Federation of June 13, 1996 No. 63-F3]. Available at: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&ts=157920527806180797367797268&cacheid=6CBBAE03A4FCF60CB46203D978DCB328&mode=splus&base=LAW&n=325409&rnd=0.32122736858355916#4obabkd24ic (assessed: 12.03.2021) (In Russ.)

11. Shamrina S.YU., Lomakina A.N. Scenarnyj analiz stress-testirovaniya pri ocenke osnovnyh vidov riskov kreditnoj organizacii [Scenario analysis of stress testing in assessing the main types of risks of a credit organization]. *Finansy i kredit*, 2018, Vol. 24, no. 7(775), pp. 1736-1750. (In Russ.)

12. Shejnov V.P. *Kak zashchitit'sya ot obmana i moshennichestva:* monogr. [How to protect yourself from fraud and fraud: monogr.] Moscow, Harvest, 2019. (In Russ.)