*Научная статья*

УДК [336.717](https://www.teacode.com/online/udc/33/336.717.html)

**Проблемы информационной безопасности в банковской сфере Российской Федерации**

***Шуть Ирина Анатольевна, Чиркова Диана Дмитриевна***

студентки 2 курса магистратуры направления «Государственный аудит» ФГБОУ «Московский государственный университет им. М.В. Ломоносова», Москва

*Original article*

**Problems of information security in the banking sector** **of the Russian Federation**

***Shut Irina Anatolyevna, Chirkova Diana Dmitrievna,***

2nd year students of the Master's degree in the direction of "State Audit" of the Moscow State University named after M.V. Lomonosov, Moscow

***Аннотация.*** В статье рассматривается значение информационной безопасности в банковской сфере, способы обеспечения и повышения уровня информационной безопасности, взаимосвязь между ростом киберпреступлений, мошенничеств с использованием цифровых технологий и ответными мерами на возникновение данных рисков, инструменты предупреждения и превентивные меры борьбы преступлениц в банковской сфере.

***Ключевые слова:*** информационная безопасность, финансовые операции, цифровые решения, банковская сфера

***Abstract.*** The article examines the importance of information security in the banking sector, ways to ensure and improve the level of information security, the relationship between the growth of cybercrime, fraud using digital technologies and responses to the occurrence of these risks, prevention tools and preventive measures to combat crimes in the banking sector.

***Keywords:*** information security, financial transactions, digital solutions, banking

**ВВЕДЕНИЕ**

Актуальность анализируемой темы связана с распространением цифровизации, цифровых решений, технологий и внедрением их в повседневную жизнь современного человека, а также ростом количества киберпреступлений. В связи с этим все больше появляется необходимость применять и совершенствовать финансовыми организациями способы обеспечения информационной безопасности.

Цель исследовательской работы **–** изучить проблемы, связанные с информационной безопасностью осуществляемых в банковской сфере операций, и определить инструменты поддержания стабильности банковской системы страны.

В рамках достижения данной цели поставлены следующие задачи:

* Выявить факторы, обуславливающие риски для банковской среды и условия для возникновения системного банковского кризиса.
* Рассмотреть механизмы противодействия мошенничеству и преступным финансовым махинациям;
* Определить инструменты и сферы их применения, способствующие обеспечению стабильности деятельности субъектов экономических отношений и построению стабильного инвестиционного климата.

Объект исследовательской работы – сфера информационной безопасности в банковском секторе.

**ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В БАНКОВСКОЙ СФЕРЕ**

Начнем с теоретического аспекта и рассмотрим официальную трактовку ключевого понятия. Согласно Стандарту Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации», под безопасностью понимается состояние защищенности интересов (целей) организации Бюджетной системы Российской Федерации в условиях угроз. Под информационной безопасностью определяется безопасность, связанная с угрозами в информационной сфере[[1]](#footnote-1).

Вострецова Е. В. под информационной безопасностью определяет «состояние защищенности информационных ресурсов (информационной среды) от внутренних и внешних угроз, способных нанести ущерб интересам организации, общества, личности и государства»[[2]](#footnote-2).

Основными компонентами информационной безопасности являются:

* доступность (обеспечение своевремнного и беспрепятсвенного доступа к информации, т.е. отсутствие угрозы отказа в обслуживании или несанкционированного использования ресурсов злоумышленниками),
* конфиденциальность (защита от несанкционированного доступа к информации, т.е. секретная информация не должна быть доступна лицу/ группе лиц, которым она не предназначена),
* целостность (непротеворечивость информации, любые изменения или удаление информации носит санкционированный характер).

Активное внедрение современных технологий дает новые возможности, но вместе с тем несет и новые угрозы – киберриски.

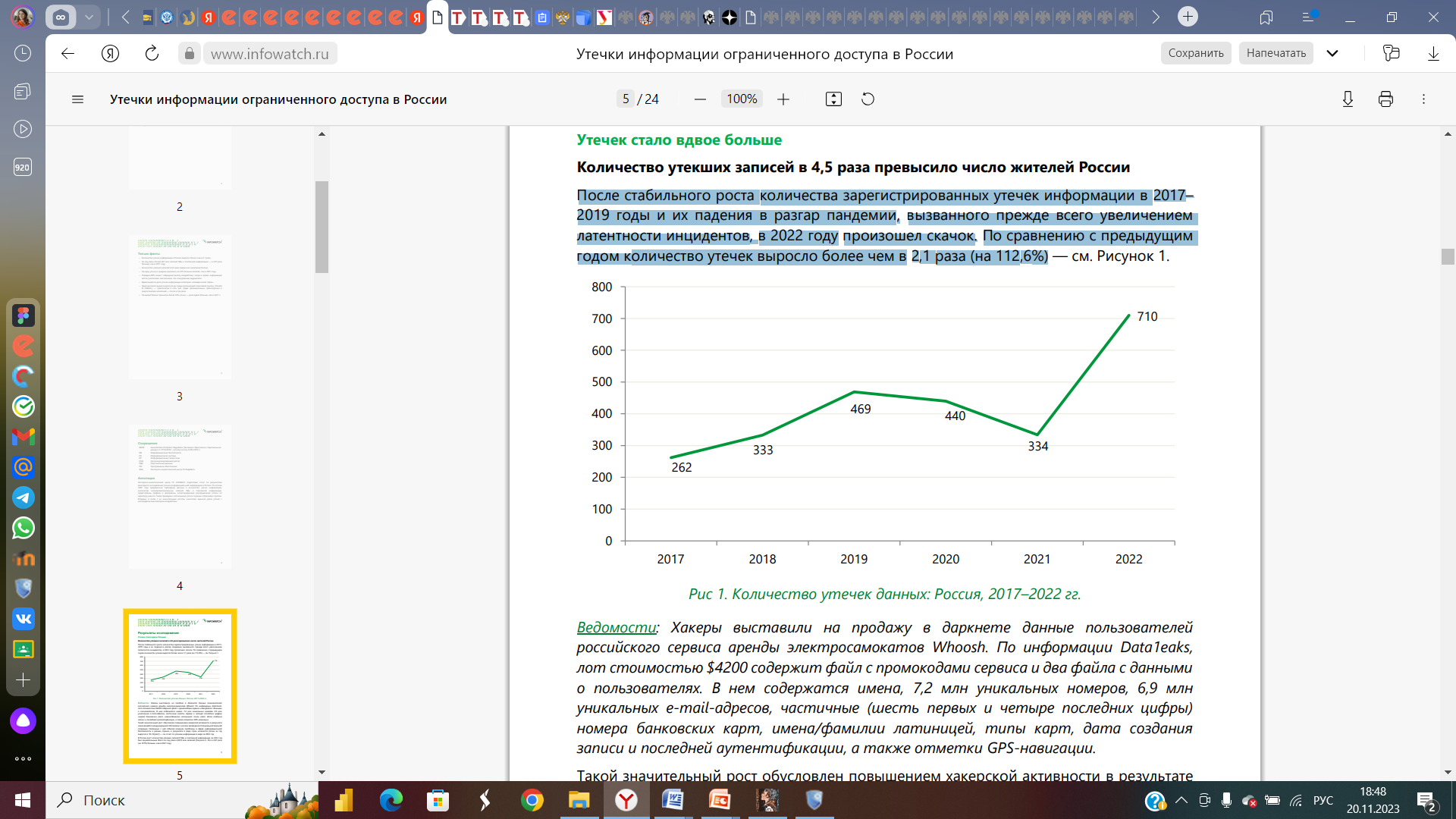
К основным киберрискам относят:

* хищение средств/персональных данных клиентов финансовых организаций,
* финансовые потери самих участников рынка,
* нарушение надежности и непрерывности предоставления финансовых услуг,
* развитие системного кризиса из-за кибератак, поразивших крупнейшие организации.

Распространение технологий открывает новые возможности, как для потребителей финансовых услуг, так и для тех, кто их предоставляет, увеличивается скорость передачи платежей, доступность получения услуг, снижение трансакционных издержек, но в тоже время новые технологии обуславливают и новые угрозы, вызовы – киберриски. Так, применение электронного документооборота и передачи данных в электронном виде оптимизирует и ускоряет многие управленческие и оптимизационные процессы, но вместе с этим и ведет к росту инцидентов несанкционного доступа к информации со стороны правонарушителей.

Процессы цифровизации стали неотъемлемой частью повседневной жизни каждого человека. Электронные ресурсы с каждым днем всё больше и больше расширяют свои границы. Так цифровизация затронула и банковскую сферу: электронный документооборот, дистанционное предоставление услуг в онлайн-формате. Однако цифровое развитие обусловило и рост цифровых мошенничеств, утечки информации в банковской сфере.

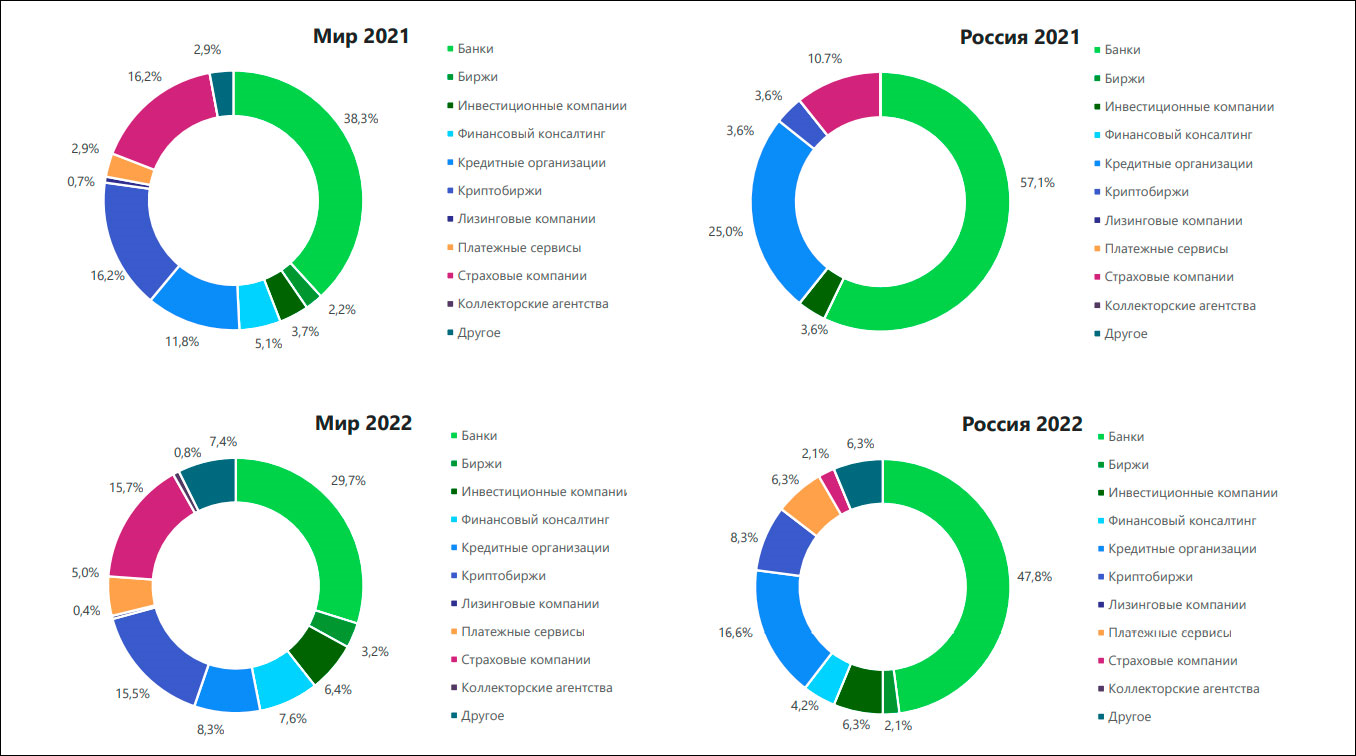
После стабильного роста количества зарегистрированных утечек информации в 2017– 2019 годы и их падения в разгар пандемии, вызванного прежде всего увеличением латентности инцидентов, в 2022 году произошел скачок. По сравнению с предыдущим годом количество утечек выросло более чем в 2,1 раза (на 112,6%) (см. график 1).



**График 1. Количество утечек данных: Россия, 2017–2022 гг.[[3]](#footnote-3)**

Отметим, что ущерб от кибератак на российскую финансовую сферу влечет за собой не только дополнительные финансовые расходы, но и отражается на имидже и репутации организаций. Так, в 2020 году Ростелеком сообщил о крупной утечки данных, которая стала самым крупным ущербом финансовой организации за год. По данным телеком-оператора, убыток более чем в 100 млн рублей был зафиксирован в двух региональных российских [банках](https://www.tadviser.ru/index.php/%D0%A4%D0%B8%D0%BD%D0%B0%D0%BD%D1%81%D0%BE%D0%B2%D1%8B%D0%B5_%D1%83%D1%81%D0%BB%D1%83%D0%B3%D0%B8,_%D0%B8%D0%BD%D0%B2%D0%B5%D1%81%D1%82%D0%B8%D1%86%D0%B8%D0%B8_%D0%B8_%D0%B0%D1%83%D0%B4%D0%B8%D1%82), не использующих системы защиты от утечек. Кроме того, кибератаки на системнообразующие банки создает не только проблемы для самой организации, но обуславливает и угрозу для безопасности и возможности надлежащего функционирования страны в целом.

Аналитики отмечают, количество утечек в российских компаниях финансового сектора за прошлый год увеличилось в 1,7 раза на фоне более значительного общемирового роста числа случаев в 3,7 раза. В общей сложности из российского финансового сектора за год утекло более 44 миллионов записей персональных данных и платежной информации, половина из которых пришлась именно на банковский сектор (порядка 48%) (см. диаграмму 1).

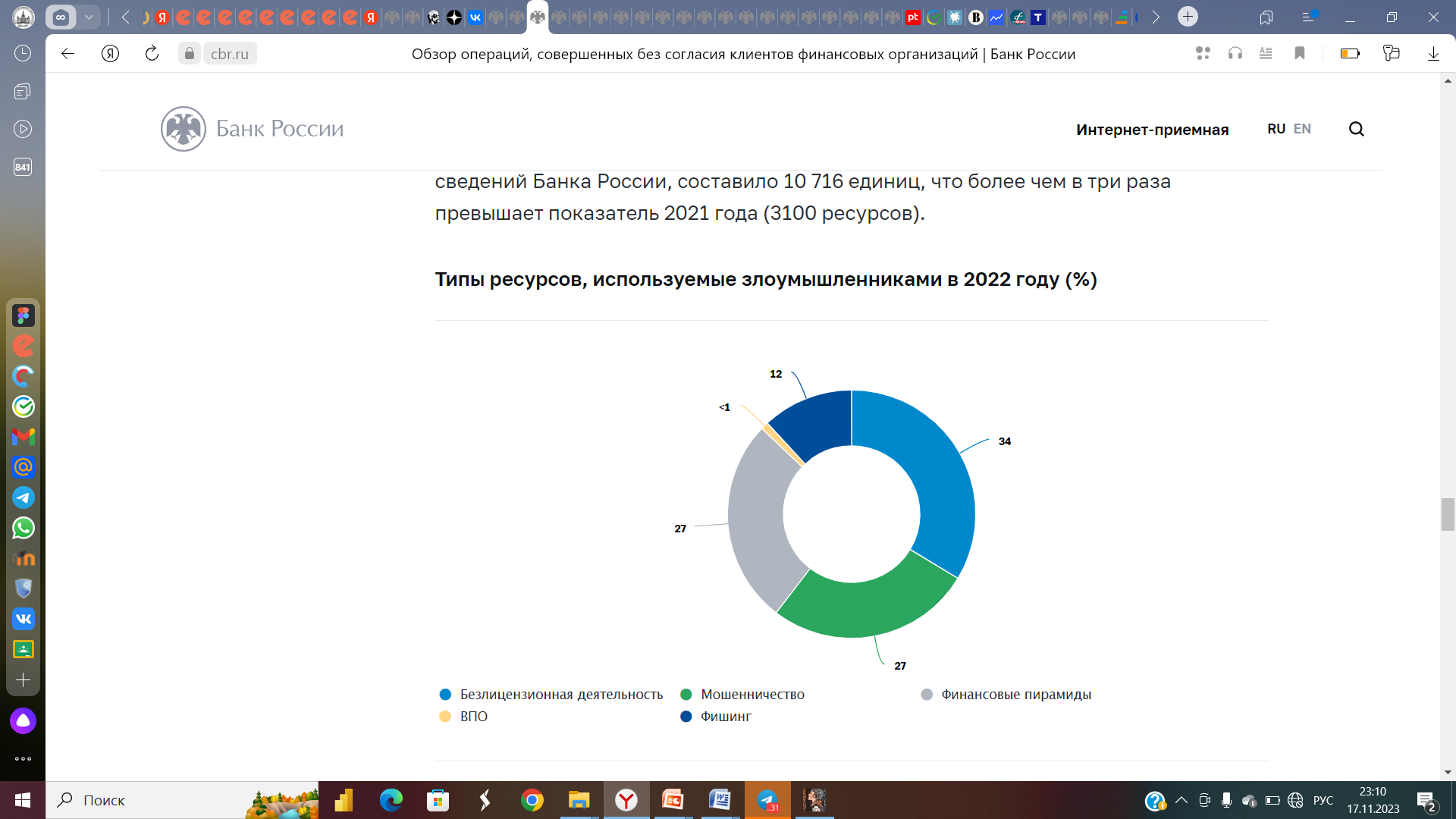


**Диаграмма 1. Утечка данных в разрезе сфер финансового спектра: Россия, 2022 гг.[[4]](#footnote-4)**

За последние годы уровень цифровых мошенничеств в финансовой сфере значительно вырос. Этому способствовал и COVID-19, обусловивший массовый переход на удаленны режим работы, и нестабильность геополитической обстановки - ввод западных санкций. По данным Центральный Банк РФ выявил, что в 1 квартале 2022 года число мошенников составило 2288, что почти втрое больше, чем в аналогичном периоде 2021 года.

Так, в 2022 году объем операций без согласия клиентов увеличился по сравнению с 2021 годом на 4,29% на фоне активного развития новых дистанционных платежных сервисов и роста объема денежных переводов (+39%, до 1458,6 трлн руб.)[[5]](#footnote-5).

На основе данных Банка России можно констатировать, что наблюдается рост мошеннических ресурсов и большую долю среди них занимает безлицензионная деятельность (операции на рынке ценных бумаг, рекламирование деятельности несуществующих кредитных, микрофинансовых и страховых организаций), мошенничество (сайты с информацией о возможности получения компенсационных выплат от государства, о возможности заработать денежные средства за прохождение опроса (теста), онлайн-кинотеатры, сайты по продаже билетов, туров и так далее) и финансовые пирамиды. Так, безлицензионная деятельность в 2022 году составила 4842 ед., против – 1825 в 2021, количество финансовых пирамид увеличилось в 4,3 раза в 2022 году, фишинг в 5,5 раза (см. диаграмму 2). Данная тенденция сохраняется по годам.



##### **Диаграмма 2. Типы ресурсов, используемые злоумышленниками в 2022 году (%)[[6]](#footnote-6).**

Регуляторы и участники финансового рынка внедряют технологии во многие сферы своей деятельности, как для целей оптимизации внутренних процедур, так и для цифровизации взаимодействия между собой. Рациональное использование технологий позволяет снизить временные и денежные затраты, повышает эффективность деятельности и качество предоставляемых услуг, обеспечивает оперативное взаимодействие, снижает риски. В рамках применения технологий регуляторами и поднадзорными организациями можно выделить два направления – SupTech и RegTech[[7]](#footnote-7).

SupTech (Supervisory Technology) – технологии, используемые регуляторами для повышения эффективности контроля и надзора за деятельностью участников финансового рынка. RegTech (Regulatory Technology) – технологии, используемые финансовыми организациями для повышения эффективности выполнения требований регулятора.

SupTech и RegTech позволяют совершенствовать сбор, обработку и анализ данных финансовых организаций, повысить качество используемых данных; совершенствовать процесс принятия решений за счет более полной и качественной аналитики; своевременно выявлять новые угрозы и уязвимости на финансовом рынке; сократить издержки поднадзорных организаций, связанных с исполнением регуляторных требований.

Отметим, что перспективным направлением, способствующим повышению финансовой безопасности, является использование искусственного интеллекта при анализе банковских операций.

Применение искусственного интеллекта при осуществлении банковских операций позволяет:

* Выявить подозрительные операции при помощи определенных признаков подозрительных операций - триггер-поинтов;
* Выявить подозрительные схемы перемещения финансов на основе анализа совокупности операций (по аналогии с риск-ориентированным подходом, применяющимся в налоговой службе);
* Автоматически выделять/ помечать красным флажком подозрительные операции и передавать их на проверку.

Можно выделить 2 модели внедрения искусственного интеллекта.

Первый вариант – ИИ будет непосредственно применяться на уровне контролирующего звена.

Второй вариант – ИИ будет применяться на банковском уровне (уже обработанные ИИ данные будут передаваться контролирующему органу).

Общим для обеих моделей будет система критериев для передачи информации. Данные должны быть четко регламентированы (объем, структура, обязательные пункты и способы их заполнения), т.е. полученная информация будет соотноситься с установленными критериями – триггер-поинтами и затем ИИ будет идентифицировать, соответствует ли она предъявляемым требованиям.

Однако применение искусственного интеллекта всегда сопряжено с риском. Так необходимо предусмотреть наличие у субъекта информационного процесса права на обжалование любых решений, принятых алгоритма ИИ, и ознакомление с данными о присвоении ему определенного статуса (например, занимаемое место в таблице по уровню рискованности осуществляемых операций).

Еще одним действенным инструментом по повышению информационной безопасности является финансовая киберграмотность. Пропаганде кибергигиены для различных категорий населения, в том числе для лиц с низким уровнем дохода и социально незащищенных категорий населения, позволит повысить безопасность предоставляемых финансовых услуг.

Таким образом, ключевыми и базовыми методами повышения информационной безопасности в банковской сфере являются:

разработка стандартов, документов и иных нормативных правовых актов, регулирующих вопросы защиты информации и определяющих политику информационной безопасности;

постоянное совершенствование кртиптографической защиты информации;

введение в практику применение мониторинга и аудита информационной безопасности в банковской сфере, позволяющих наблюдать, анализировать и оценивать угрозы воздействия мошенников.

**ЗАКЛЮЧЕНИЕ**

Активное развитие цифровых технологий значительно изменило потребности и  ожидания получателей финансовых услуг. Клиенты хотят получать широкий спектр услуг, предпочитая простые и быстрые сервисы, в которых не нужно повторно проходить авторизацию и вводить свои личные данные. Однако ускоренное развитие технологий создает и существенные риски кибератак на клиентов и финансовые организации, а также мошенничества на финансовом рынке.

Повсеместное внедрение цифровых технологий в целях противодействия нелегальным финансовым операциям позволит своевременно обнаруживать, выявлять и снижать риски реализации незаконных финансовых сделок. С этой целью необходимо сформировать условия для обеспечения информационной безопасности и киберустойчивости цифровых и платежных технологий через регулирование и их последующий надзор, а также формирование устойчивой национальной платежной инфраструктуры.

Безусловно, попытки поиска путей минимизации киберпреступлений на территории Российской Федерации ведутся достаточно активно, так в 2015 г. приняты и введены в действия Приказом Банка России рекомендации «Обеспечение информационной безопасности организаций банковской системы РФ», согласно которому организациям необходимо:

– разделять потоки информации и изолировать виртуальные машины;

– проводить мониторинги информационной безопасности;

– обеспечивать информационную безопасность в системе хранения данных[[8]](#footnote-8).

В связи с этим необходимо:

* дальнейшее совершенствование системы внешнего аудита информационной безопасности за счет RegTech- и SupTech-проектов;
* внедрение системы мониторинга и анализа операционных рисков кредитных организаций (переход к системному использованию методов продвинутой аналитики);
* интегрировать результаты мониторинга и анализа операционных рисков кредитных организаций в оценку экономического положения, планов восстановления финансовой устойчивости, а также качества внутренних процедур оценки достаточности капитала кредитных организаций;
* распространение киберучения в целях обеспечения операционной надежности кредитных организаций;
* создание условий для безопасности хранения конфиденциальных данных, а также регулярное изменение и проверка кодов доступа и паролей.

Из-за возрастания числа цифровых мошенничеств, организациям в банковской сфере необходимо уделить особенно пристальное внимание защите данных и обеспечению информационной безопасности. Поскольку дальнейшее развитие экономики в современном мире, в особенности ее фундамента – финансовой сферы, в частности – банков, невозможно без понимания сущности информационной безопасности. Соответственно, необходимо совершенствование правовой базы; построение институциональных составляющих государственной политики в сфере информационной безопасности; снабжение необходимыми программным обеспечением, оборудованием, сервисами и иными ресурсами банков; разработка превентивных мер по выявлению угроз и пресечению кибератак.

**Список источников**

Стандарт Банка России СТО БР ИББС-1.0–2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации/ Общие положения» (принят и введен в действие распоряжением Банка России от 17 мая 2014 г. № Р-399). [Электронный ресурс] – Режим доступа: <https://www.consultant.ru/document/cons_doc_LAW_163762/> (дата обращения: 18.11.2023)

Обзор операций, совершенных без согласия клиентов финансовых организаций. [Электронный ресурс] – Режим доступа: https://cbr.ru/analytics/ib/operations\_survey\_2022/ (дата обращения: 18.11.2023)

Основные направления развития технологий suptech и regtech на период 2021–2023 годов. [Электронный ресурс] – Режим доступа: https://cbr.ru/Content/Document/File/120709/SupTech\_RegTech\_2021-2023.pdf (дата обращения: 18.11.2023)

1. Основы информационной безопасности: учебное пособие для студентов вузов / Е.В. Вострецова. – Екатеринбург : Изд-во Урал. унивеситета, 2019. – 204 с.

Проблемы обеспечения информационной безопасности в банковской сфере Российской Федерации [Электронный ресурс] – Режим доступа: <https://www.elibrary.ru/download/elibrary_41443803_96548592.pdf> (дата обращения: 18.11.2023)

Проблемы управления информационной безопасностью информационных систем организаций кредитно-банковской сферы [Электронный ресурс] – Режим доступа: <https://www.elibrary.ru/download/elibrary_54286750_24200875.pdf> (дата обращения: 18.11.2023)

Рекомендации в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы РФ. Обеспечение информационной безопасности при использовании технологии виртуализации» [РС БР ИББС-2.8-2015](https://www.consultant.ru/document/cons_doc_LAW_178184/). [Электронный ресурс] – Режим доступа: http://www.consultant.ru/law/hotdocs/42406.html?utm\_campaign= hotdocs\_day11 (дата обращения: 18.11.2023)

Россия: утечки информации ограниченного доступа в 2022 г., Экспертно-аналитический центр InfoWatch. 2023 г. [Электронный ресурс] – Режим доступа: https://www.infowatch.ru/sites/default/files/analytics/files/utechki-informatsii-ogranichennogo-dostupa-v-rossii-za-2022-god.pdf?ysclid=lp72xts8ll440256778 (дата обращения: 18.11.2023)

**References**

1. Standard of the Bank of Russia STO BR IBBS-1.0–2014 "Ensuring information security of organizations of the banking system of the Russian Federation/ General Provisions" (adopted and put into effect by the Order of the Bank of Russia dated May 17, 2014 No. R-399). [Electronic resource] – Access mode: https://www.consultant.ru/document/cons\_doc\_LAW\_163762 / (accessed: 11/18/2023)

2. Review of transactions performed without the consent of clients of financial institutions. [Electronic resource] – Access mode: https://cbr.ru/analytics/ib/operations\_survey\_2022 / (accessed: 11/18/2023)

3. The main directions of development of suptech and regtech technologies for the period 2021-2023. [Electronic resource] – Access mode: https://cbr.ru/Content/Document/File/120709/SupTech\_RegTech\_2021-2023.pdf (accessed: 11/18/2023)

4. Fundamentals of information security: a textbook for university students / E.V. Vostretsova. – Yekaterinburg : Ural Publishing House. university, 2019. – 204 p.

5. Problems of ensuring information security in the banking sector of the Russian Federation [Electronic resource] – Access mode: https://www.elibrary.ru/download/elibrary\_41443803\_96548592.pdf (accessed: 11/18/2023)

6. Problems of information security management of information systems of credit and banking organizations [Electronic resource] – Access mode: https://www.elibrary.ru/download/elibrary\_54286750\_24200875.pdf (accessed: 11/18/2023)

7. Recommendations in the field of standardization of the Bank of Russia "Ensuring information security of organizations of the banking system of the Russian Federation. Ensuring information security when using virtualization technology" RS BR IBBS-2.8-2015. [Electronic resource] – Access mode: http://www.consultant.ru/law/hotdocs/42406.html?utm\_campaign = hotdocs\_day11 (accessed: 11/18/2023)

8. Russia: leaks of restricted access information in 2022, Expert Analytical Center InfoWatch. 2023 [Electronic resource] - Access mode: https://www.infowatch.ru/sites/default/files/analytics/files/utechki-informatsii-ogranichennogo-dostupa-v-rossii-za-2022-god.pdf?ysclid=lp72xts8ll440256778 (accessed: 11/18/2023)

1. Стандарт Банка России СТО БР ИББС-1.0–2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации/ Общие положения» (принят и введен в действие распоряжением Банка России от 17 мая 2014 г. № Р-399). URL - https://www.consultant.ru/document/cons\_doc\_LAW\_163762/ [↑](#footnote-ref-1)
2. Основы информационной безопасности : учебное пособие для студентов вузов / Е.В. Вострецова. – Екатеринбург: Изд-во Урал. унивеситета, 2019. – 204 с. [↑](#footnote-ref-2)
3. Россия: утечки информации ограниченного доступа в 2022 г., Экспертно-аналитический центр InfoWatch. 2023 г. URL - https://www.infowatch.ru/sites/default/files/analytics/files/utechki-informatsii-ogranichennogo-dostupa-v-rossii-za-2022-god.pdf?ysclid=lp72xts8ll440256778 [↑](#footnote-ref-3)
4. Там же. [↑](#footnote-ref-4)
5. # Обзор операций, совершенных без согласия клиентов финансовых организаций. URL - https://cbr.ru/analytics/ib/operations\_survey\_2022/

   [↑](#footnote-ref-5)
6. Там же. [↑](#footnote-ref-6)
7. Основные направления развития технологий suptech и regtech на период 2021–2023 годов. URL - https://cbr.ru/Content/Document/File/120709/SupTech\_RegTech\_2021-2023.pdf [↑](#footnote-ref-7)
8. Рекомендации в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы РФ. Обеспечение информационной безопасности при использовании технологии виртуализации» [РС БР ИББС-2.8-2015](https://www.consultant.ru/document/cons_doc_LAW_178184/). URL - http://www.consultant.ru/law/hotdocs/42406.html?utm\_campaign= hotdocs\_day11 [↑](#footnote-ref-8)