УДК 336.71: 004.056
DOI: 10.34020/1993-4386-2025-1-36-43

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В БАНКАХ

Т. Б. Кувалдина, А. А. Срибная
Омский государственный университет путей сообщения (ОмГУПС),
Омск, Россия

В статье рассматриваются ключевые аспекты информационной безопасности банков в Российской Федерации, акцентируется внимание на актуальных угрозах и вызовах, с которыми сталкиваются финансовые организации. Исследуется современное состояние систем мер, направленных на обеспечение конфиденциальности, целостности и доступности информации в контексте быстро меняющегося киберугрозного ландшафта на основании статистики утечек данных, происходящих в банковской сфере за последние годы. Полученные материалы подчеркивают масштабы проблемы и ставят перед институтами финансовой сферы задачу по улучшению мер безопасности. В статье даны рекомендации по укреплению информационной безопасности банков и повышению уровня защиты персональных данных клиентов, что является критически важным для сохранения доверия со стороны пользователей и устойчивости финансовой системы в целом.

Ключевые слова: банки, безопасность, информационная безопасность, конфиденциальная информация, утечка данных.

В цифровом обществе становится очевидным, что для конструирования и продажи безопасных банковских продуктов важно обеспечивать высокий уровень информационной безопасности (ИБ). Отечественные банки в настоящее время поддерживают связи между различными отраслями и сегментами экономики, а также с конечными потребителями товаров и услуг, что делает их деятельность уязвимой со стороны киберпреступников по нескольким причинам. Во-первых, из года в год увеличивается масштаб электронной инфраструктуры в банковской системе, которая, с одной стороны, должна обеспечивать стабильную работу онлайн-платформ, масштабируемость бизнеса, с другой стороны, становится весьма уязвимой для хакерских атак. Во-вторых, использование всеми субъектами рынка электронных платежных систем влияет на их экономическую деятельность и усиливает опасность мошеннических действий. В-третьих, уход из России иностранных производителей технологий по кибербезопасности и трудности в получении обновлений по ним ослабили защитный периметр банков и усилил, интерес со стороны хакеров.

По мнению М. Н. Мельник и О. В. Мадатова, в основе общей оценки угроз безопасности любого банка лежит соблюдение обязательных нормативов и стандартов, «нарушение каждого из которых создает реальную угрозу самому существованию банка по причине появления оснований для приостановления или отзыва у него лицензии, следствием чего является неминуемое банкротство» [1]. Причем, среди основных показателей, оценивающих эффективность деятельности банка по противодействию информационным угрозам, авторы указывают: общую продолжительность ограничения удаленного доступа клиентов к информационным ресурсам банка; наличие утечки личных данных и сведений, составляющих банковскую тайну; финансовые потери банка в результате нарушений информационной безопасности» [1].

В. О. Одинцов утверждает, что в «условиях повсеместного распространения новых технологий, которые закрепились, в том числе и в банковской сфере, первоочередной целью в рамках обеспечения безопасности становится безопасность информационная» [2].

С точки зрения Н. В. Фадейкиной, обеспечение информационной безопасности банка – «это непрерывный системно-обеспечивающий процесс, который направлен на предотвращение возможных угроз финансовых потерь и репутационных рисков в целях обеспечения устойчивого развития банка в долгосрочной перспективе» [3].

Чтобы обеспечить высокий уровень информационной безопасности в банковской сфере, нужно во время идентифицировать возможную опасность и оперативно принимать решительные действия, способные минимизировать реальные угрозы.

Однако обеспечение ИБ в банках не простая задача, а сложный процесс, требующий определенных усилий и навыков большого количества специалистов, а также серьезной сетевой защиты информации.

С каждым годом банки внедряют большое количество инновационных банковских продуктов, расширяют перечень оказываемых услуг, что вызывает необходимость разработки и принятия единых методов и норм, применяемых при оценке ИБ. Это будет только способствовать укреплению банковской системы.

При разработке комплекса организационных и технических мер, направленных на защиту личных данных клиентов банков, нужно исходить из следующих соображений:

– информация о сделках, операциях граждан и юридических лиц, находящаяся в распоряжении банков, эквивалентна деньгам; доступ к сведениям, который не обеспечивает их защиту, может привести к опасным угрозам, приводящим к существенным финансовым потерям;

– банки хранят информацию о большом количестве своих клиентов, поэтому обеспечение адекватной безопасности должно оставаться приоритетной задачей;

– удобство обслуживания клиентов и широкий спектр услуг напрямую влияют на конкурентоспособность банка, что делает важным быстрый и безопасный доступ к финансовым ресурсам; однако это также увеличивает риски для систем безопасности;

– банк несет ответственность за сохранность не только своих финансов, но и средств клиентов, и должен обеспечить высокую надежность применяемых информационных систем даже в условиях инцидентов;

– хранение важной информации о клиентах приводит к увеличению числа угроз со стороны злоумышленников.

В целях минимизации киберугроз в России был разработан нормативный документ, содержащий комплекс норм по защите банковской системы, ориентированный на требования международного регулятора. Указанный стандарт содержит в себе описание пяти этапов создания системы обеспечения ИБ, от разработки её политики до контроля реализации (рис. 1).

Самым значимым этапом в формировании системы обеспечения ИБ является оценка рисков, которая заключается в идентификации опасности для информационной системы и её ресурсов. Итоги этой оценки включают описание угроз, уязвимостей и потенциальных последствий, что позволяет выбрать адекватные меры для обеспечения желаемого уровня безопасности (рис. 2).

Рис. 1. Процесс конструирования системы обеспечения информационной безопасности

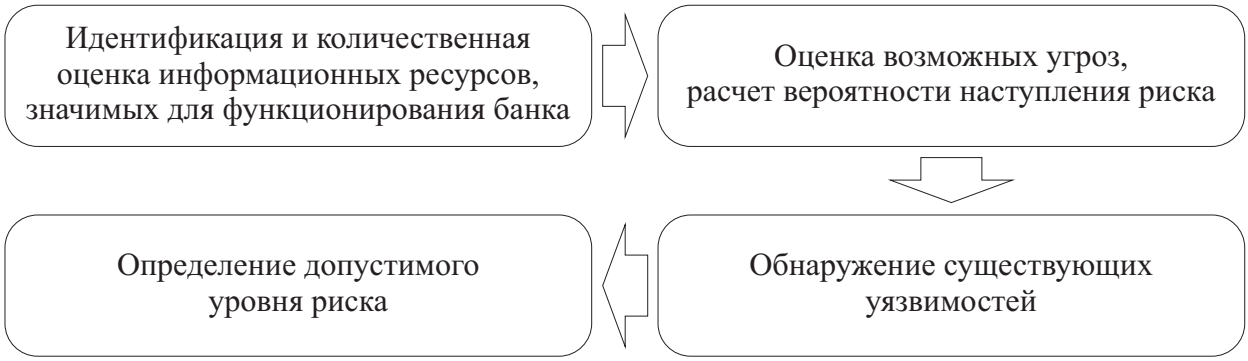

Рис. 2. Алгоритм оценки рисков информационной безопасности

Доступность информации, в том числе при осуществлении финансовых операций, показывает возможность реализации пользователями своих прав доступа. Но при этом они должны быть уверены в том, что их персональные данные будут целостными и конфиденциальными. Как считают Р. Х. Марданов и И.В. Ильин, целостность данных показывает их неизменность при выполнении операций с ними, будь то передача, использование или хранение информации [4]. Конфиденциальность идентифицируется как свойство безопасности информации.

К необходимым условиям непрерывности банковского бизнеса, как и любого другого, следует отнести обеспечение таких принципов, как конфиденциальность, целостность и доступность информации; реализация указанных принципов в системе обеспечения ИБ в банке достаточно сложна, многое зависит от уровня зрелости процессов управления ИБ (рис. 3).

Неполный процесс: управление ИБ отсутствует или рассматривается только как техническая проблема.

Осуществленный процесс: процесс внедрен, но не стандартизирован; понимание важности ИБ начинает формироваться.

Управляемый процесс: внедрение управления процессом; разработаны концепция и политика ИБ.

Установленный процесс: управляемый процесс стандартизирован и задокументирован; разработаны методики анализа рисков.

Предсказуемый процесс: процессы находятся в стадии непрерывного совершенствования, внедряются методы для лучшего обнаружения и реагирования на угрозы.

Оптимизируемый процесс. Защитные меры в организации применяются комплексно, что обеспечивает их эффективность. Организация быстро адаптируется к изменениям во внешней среде и бизнесе.

Рис. 3. Уровни зрелости процессов управления информационной безопасностью

Как показывает практика, уровень зрелости процессов управления ИБ зависит от соблюдения субъектами банковской системы Российской Федерации (БС РФ) установленных Банком России стандартов, даже если стандарты носят рекомендательный характер.

Еще в 2012 г. П. В. Ревенков отмечал следующее: «Стандарты образуют понятийный базис, на котором строятся все работы по обеспечению ИБ, и определяют критерии, которым должно следовать управление ИБ. Банк России давно определил проблему обеспечения ИБ как одну из основных составляющих стабильности банковской системы. Начиная с 2004 г. регулятор приступил к выпуску общекорпоративных стандартов по ИБ» [5].

В 2014 г. Банком России введен Стандарт СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации/ Общие положения». Его целями «являются развитие и укрепление БС РФ, повышение доверия к БС РФ, поддержание стабильности организаций БС РФ и на этой основе – стабильности БС РФ в целом, достижение адекватности мер защиты реальным угрозам ИБ; предотвращение и (или) снижение ущерба от инцидентов ИБ, а основными задачами – установление единых требований по обеспечению ИБ организаций БС РФ, а также повышение эффективности мероприятий по обеспечению и поддержанию ИБ организаций БС РФ».

В рассматриваемом Стандарте подчеркнуто, что «группы процессов системы менеджмента информационной безопасности (СМИБ) организации БС РФ следует организовывать в виде циклической модели Деминга "... – планирование – реализация – проверка – совершенствование – планирование – ... ", которая является основой модели менеджмента стандартов качества ГОСТ Р ИСО 9001 и ИБ ISO/IEC IS 27001. Организация и выполнение процессов СМИБ необходимы в том числе для обеспечения уверенности в том, что хороший практический опыт банка документируется, становится обязательным к применению, а СМИБ совершенствуется.

Безопасность банков всегда была одной из самых обсуждаемых тем, особенно в свете современных угроз кибербезопасности, поскольку банк – это денежно-кредитный институт, где хранятся не только деньги клиентов, но и их персональные данные. С увеличением числа онлайн-транзакций и цифровых услуг важность защиты этой информации возрастает в разы.

Исходя из того, что «развитие и укрепление БС РФ, а также обеспечение эффективного и бесперебойного функционирования платежной системы РФ являются целями деятельности Банка России, важнейшим условием реализации этих целей становится обеспечение необходимого и достаточного уровня ИБ организаций БС РФ, их активов (в том числе информационных), который во многом определяется уровнем ИБ банковских технологических процессов (платежных, информационных и др.). Однако особенности банковских систем таковы, что негативные последствия сбоев в работе отдельных организаций могут привести к быстрому развитию системного кризиса платежной системы РФ, нанести ущерб интересам собственников и клиентов. В случаях наступления инцидентов ИБ значительно возрастают результирующий риск и возможность нанесения ущерба организациям БС РФ. Поэтому для организаций БС РФ угрозы информационным активам, то есть угрозы ИБ, представляют реальную опасность» [].

К сожалению, несмотря на все усилия и осуществляемые инвестиции в ИБ, потребители финансовых услуг все чаще сталкиваются с инцидентами утечки данных. Взломы и кибератаки становятся обыденностью, и банки, как и другие организации, оказываются под угрозой. Так, например, утечка личных данных клиентов может не только вызвать финансовые потери, но и подорвать доверие к финансовым организациям в целом.

Незаконное получение доступа к конфиденциальной, личной информации лицом, не имеющим соответствующего разрешения, в мире растет[1] (рис. 4).

По данным экспертно-аналитического центра InfoWatch, в 2023 году было обнаружено 1 049 утечек секретной информации из финансовых организаций. Это почти на 80 % больше, чем в 2022 году. По сравнению с 2021 годом, продемонстрирован ещё более значительный рост (в 6,7 раза)[2].

Киберпреступники незаконно входят в интегрированную информационную сеть компаний, предназначенную для обмена данными, используя вредоносное программное обеспечение (ПО), например, вирусы, ботов, программу-шпиона и др. Российская федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) подтвердила утечку данных клиентов МТС-банка и составила административный протокол о нарушении законодательства в области персональных данных. В частности, злоумышленниками были похищены такие сведения, как ФИО, даты рождения, пол, гражданство и ИНН[3].

[1] Побиты все рекорды по числу утечек данных. В интернет утекло 286 млн телефонных номеров и 96 млн электронных почт (публикация от 22.10.2024 г.). URL: https://www.cnews.ru/news/top/2024-10-22_sektor_elektronnoj_kommertsii (дата обращения: 22.01.2025).

[2]. Там же.

[3] Утечки данных в финансовом секторе выросли в 3,2 раза (публикация от 16.02.2024 г.) / Национальный банковский журнал. URL: https://nbj.ru/publs/utechki_dannykh_v_finansovom_sektore_vyros/ 64637/ (дата обращения 22.10.2024) (дата обращения: 22.01.2025).

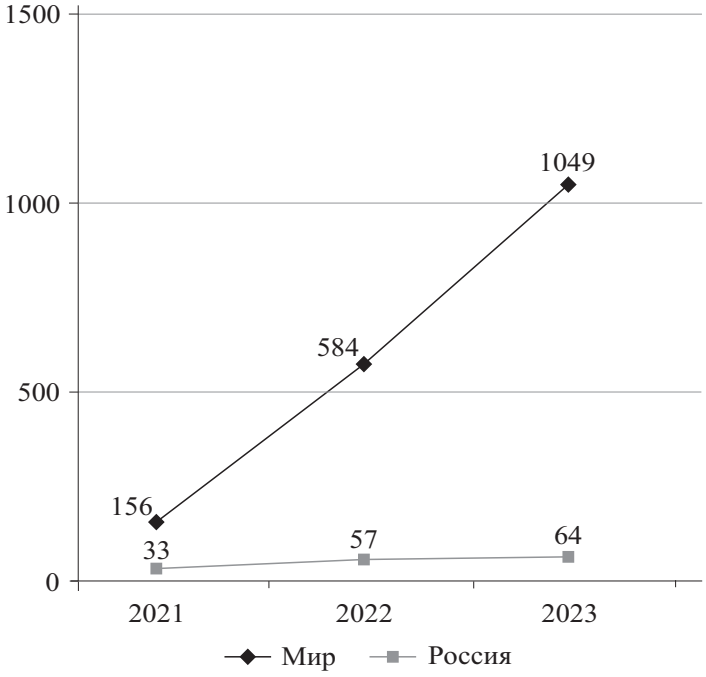

Рис. 4. Количество утечек конфиденциальной информации из организаций в отрасли «Банки и финансовые услуги»

Следует отметить, что хакеры постоянно совершенствуют схемы и методы обмана граждан, используя не только технические средства, но и применяя психологическое манипулирование людьми с целью совершения противоправных действий. На рисунках 5 и 6 графически изображено количество утечек с учётом новых обнаруженных случаев компрометации данных в 2021–2022 годах, начиная с 1 февраля 2023 года (ряд 1) и до 1 февраля 2024 года (ряд 2)[4].

Интерес вызывает информация об утечке данных в финансовом секторе по типам инцидентов в мире[5] (рис. 7).

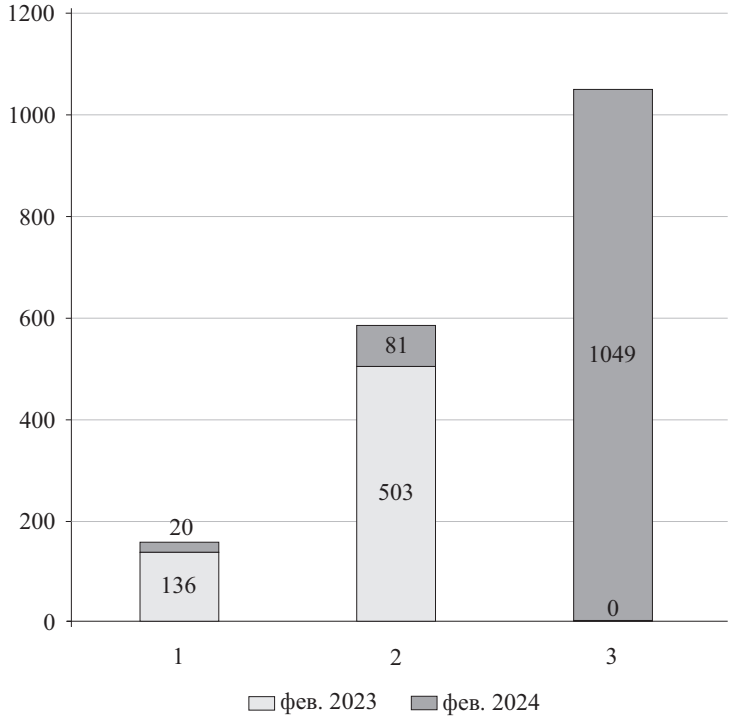

Рис. 5. Утечки данных в финансовом секторе, глобальный мир

[4] Киберугрозы финансовой отрасли: промежуточные итоги 2023 года (публикация от 09.11.2023 г.). URL: https://www.ptsecurity.com/ru-ru/research/analytics/financial-industry-security-interim-2023/ (дата обращения: 25.01.2025).

[5] Там же.

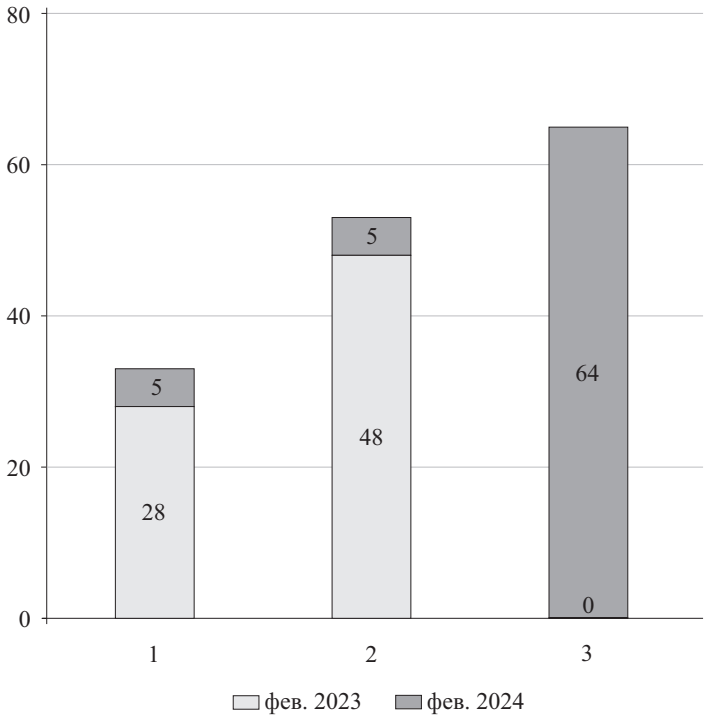

Рис. 6. Утечки данных в финансовом секторе, Россия

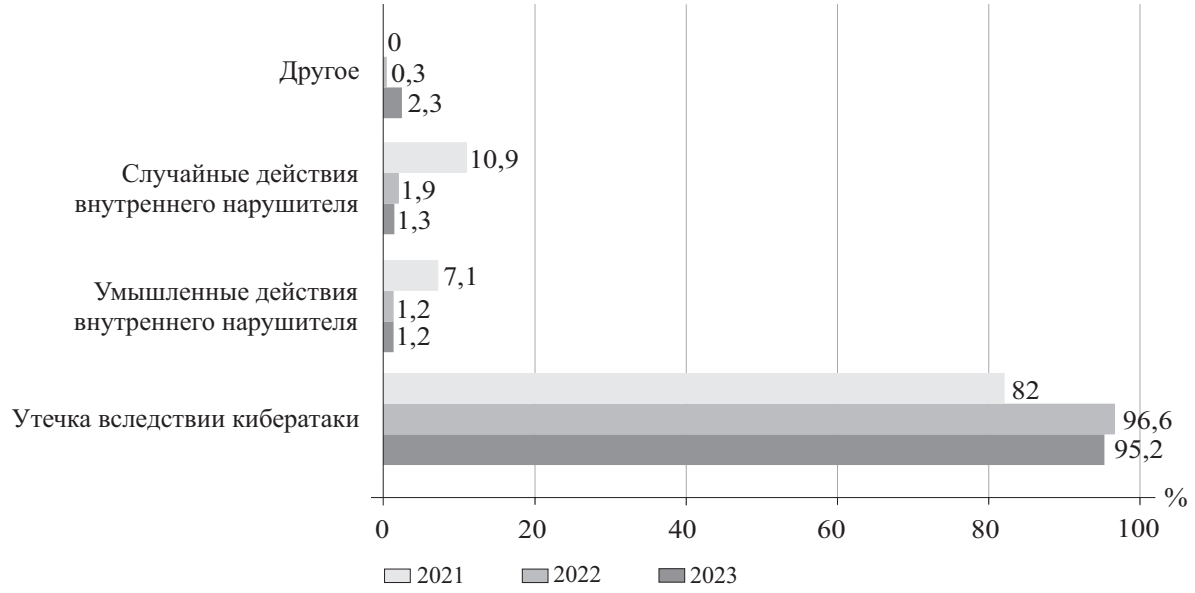

Рис. 7. Потеря информации в финансовом секторе по типам инцидентов, мир

Практика свидетельствует, что именно кибератаки являются виной утечки ценной информации в финансовом секторе. На их долю в мире приходится 96 %. Россия не является исключением[6] (рис. 8).

Большая часть преступлений в сфере компьютерной информации вызваны умышленными действиями. Речь идет не только о России. В большинстве стран мира складывается похожая ситуация. Это говорит о серьезной угрозе, с которой сталкивается общество.

Особые опасения вызывает тот факт, что противоправные действия порой совершаются с участием работников финансовых организаций, в том числе банков. Данные статистики свидетельствуют, что доля таких происшествий, формально снизилась, до 2,5 % в мире и до 6,3 % в России. Можно выделить несколько причин, почему это произошло. Во-первых, банки

[6] Там же.

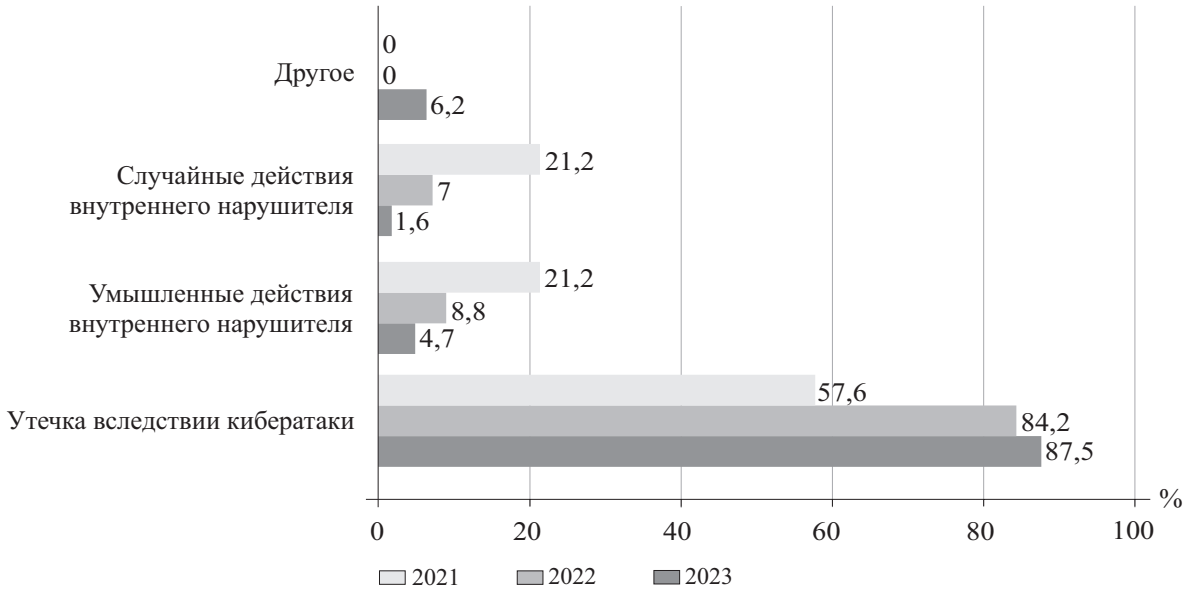

Рис. 8. Потеря информации в финансовом секторе по типам инцидентов, Россия

уделяют большое внимание профилактике внутренних нарушений со стороны своих работников, используя более эффективные DLP-системы нового поколения и психодиагностику, инновационное оборудование и ПО в целях контроля перемещения и доступа в помещения сотрудников. Во-вторых, по оценкам экспертов, увеличилась скрытность злонамеренных действий сотрудников: взаимодействие внутренних и внешних нарушителей (так называемый «гибридный вектор» атак)[7].

В целях обеспечения высокого уровня ИБ, организации принимают различные меры. Но, по мнению работников, участвующих в опросе, наибольшую эффективность показали мероприятия по проведению обучающихся семинаров (42% ответивших) и внедрение DLP (33 % ответивших).

Итак, проведенное исследование позволили констатировать, что современные банки сталкиваются с возрастающим количеством киберугроз, что требует постоянного обновления и совершенствования систем защиты информации. Кроме того, требуется пересмотреть кадровую политику банков, которая должна формировать высококвалифицированный кадровый потенциал, обеспечивающий гарантированное достижение запланированных результатов, в том числе по защите личных данных клиентов. При этом, особое внимание следует уделить соблюдению работниками банков этических норм и правил служебного поведения, проверяя их на добросовестность и честность.

Статистика неправомерного завладения конфиденциальной информацией лицом, не имеющим соответствующего разрешения, свидетельствует, что уязвимости в системе безопасности часто становятся причиной серьезных инцидентов, наносящих вред, как самим финансовым организациям, так и их клиентам. При этом стоит признать тот факт, что сами клиенты порой передают злоумышленникам свои персональные данные, поддаваясь на их угрозы и шантаж. В основном попадает на уловки мошенников пожилое население страны. Поэтому стоит продолжить просветительскую работу с людьми предпенсионного и пенсионного возраста через структурные подразделения банков, сервис «Госуслуги» и домовые чаты.

Литература

1. *Мельник М. Н., Мадатова О. В.* Анализ угроз экономической безопасности кредитной организации / В сборнике: Современные научные исследования: исторический опыт и инновации // Сборник материалов XIX Международной (политематической) научно-практической конференции (Краснодар, 09–10 февраля 2023 г.). – Краснодар: Академия маркетинга и социально-информационных технологий – ИМСИТ, 2023. С. 318–323.

2. *Одинцов В. О.* Современные инструменты обеспечения экономической безопасности коммерческого банка / В сборнике: Теоретические и прикладные вопросы экономики, управления и образования // Сборник статей IV Международной научно-практической конференции (Пенза, 13–14 июня 2023 г.). Под научной редакцией Б. Н. Герасимова. – Пенза: Пензенский государственный аграрный университет, 2023. С. 267–271.

3. *Фадейкина Н. В., Зырянов В. С.* Информационная и экономическая безопасность кредитной организации как факторы обеспечения ее устойчивого развития // Сибирская финансовая школа. 2024. № 2 (154). С. 50-60.

4. *Марданов Р. Х., Ильин И. В.* Стандарты информационной безопасности в банковской системе // Вестник Уфимского государственного авиационного технического университета. 2013. Т. 17, № 7 (60). С. 55–60.

[7] Утечки данных из банков России (публикация от 20.02. 2025 г.). URL: https://www.tadviser.ru/index. php/Статья:Утечки_данных_из_банков_России (дата обращения 22.02.2025).

5. *Ревенков П. В.* Обеспечение информационной безопасности в условиях интернет-банкинга // Экономические стратегии. 2012. Т. 14, № 3 (101). С. 104–112.

6. *Сердюк В.* Роль стандартов Банка России в обеспечении информационной безопасности кредитно-финансовых организаций // Бухгалтерия и банки. 2008. № 3. С. 36–42.

Сведения об авторах

Кувалдина Татьяна Борисовна – член Редакционной коллегии научного журнала «Сибирская финансовая школа», доктор экономических наук, доцент, профессор кафедры «Экономическая безопасность и управление финансами», Омский государственный университет путей сообщения (ОмГУПС), Омск, Россия.
Email: kuvaldina2004@mail.ru

Срибная Александра Алексеевна – студент факультета информационной безопасности Омского государственного университета путей сообщения (ОмГУПС), Омск, Россия.
E-mail: sribnaj2003@gmail.com

INFORMATION SECURITY IN BANKS

T. Kuvaldina, A. Sribnaya
Omsk State Transport University (OSTU),
Omsk, Russia

The article examines the key aspects of information security of banks in the Russian Federation, focuses on the current threats and challenges faced by financial institutions. The article examines the current state of systems of measures aimed at ensuring confidentiality, integrity and accessibility of information in the context of a rapidly changing cyber threat landscape based on statistics of data leaks occurring in the banking sector in recent years. The materials received highlight the scale of the problem and set financial institutions the task of improving security measures. The article provides recommendations on strengthening the information security of banks and improving the protection of personal data of customers, which is crucial for maintaining user trust and the stability of the financial system as a whole.

Keywords: banks, security, information security, confidential information, data leakage.

References

1. Mel'nik M. N., Madatova O. V. Analysis of threats to the economic security of a credit institution, *Sovremennye nauchnye issledovaniya: istoricheskii opyt i innovatsii* [Modern scientific research: historical experience and innovations], Collection of materials of the XIX International (political) scientific and practical conference (Krasnodar, February 09-10, 2023), Krasnodar: Akademiya marketinga i sotsial'no-informatsionnykh tekhnologii, IMSIT, 2023, pp. 318–323. (In Russ.).

2. Odintsov V. O. Modern tools for ensuring the economic security of a commercial bank, *Teoreticheskie i prikladnye voprosy ekonomiki, upravleniya i obrazovaniya* [Theoretical and applied issues of economics, management and education], Collection of articles of the IV International Scientific and Practical Conference (Penza, June 13-14, 2023), Penza: Penzenskii gosudarstvennyi agrarnyi universitet, 2023, pp. 267–271. (In Russ.).

3. Fadeikina N. V., Zyryanov V. S. Information and economic security of a credit institution as factors of ensuring its sustainable development, *Sibirskaya finansovaya shkola*, 2024, No. 2 (154), pp. 50-60. (In Russ.).

4. Mardanov R. Kh., Il'in I. V. Information security standards in the banking system, *Vestnik Ufimskogo gosudarstvennogo aviatsionnogo tekhnicheskogo universiteta*, 2013, Vol. 17, No. 7 (60), pp. 55–60. (In Russ.).

5. Revenkov P. V. Ensuring information security in the context of online banking, *Ekonomicheskie strategii*, 2012, Vol. 14, No. 3 (101), pp. 104–112. (In Russ.).

6. Serdyuk V. The role of the Bank of Russia standards in ensuring the information security of financial institutions, *Bukhgalteriya i banki*, 2008, No. 3, pp. 36–42. (In Russ.).

About the authors

Tatyana B. Kuvaldina – Member of the Editorial Board of the scientific journal «Siberian Financial School», Doctor of Economics, Professor of the Department of Economic Security and Financial Management, Omsk State University of Railway Engineering (OmGUPS) Omsk, Russia.
Email: kuvaldina2004@mail.ru

Alexandra A. Sribnaya – student of the Faculty of Information Security of Omsk State University of Communications (OmGUPS), Omsk, Russia.
E-mail: sribnaj2003@gmail.com