УДК 336:004.056
DOI: 10.34020/1993-4386-2024-3-20-27

КИБЕРБЕЗОПАСНОСТЬ В ФИНАНСОВОМ СЕКТОРЕ ЭКОНОМИКИ: НЕОБХОДИМОСТЬ И ЗНАЧИМОСТЬ

К. Е. Следнева, Т. Б. Кувалдина
Омский государственный университет путей сообщения (ОмГУПС),
Омск, Россия

В век развития технологий, финансовый сектор экономики России один из первых активно начал переход на цифровую трансформацию всех бизнес-процессов. Для ускорения проведения финансовых операций и повышения качества финансовых услуг стали использоваться электронные платформы. Население страны все активнее переходит на безналичные расчеты при оплате товаров, работ и услуг. У россиян появилась возможность приобретать цифровые активы через банковскую карту на самых разных электронных ресурсах, не выходя из дома. Тем не менее, наряду с плюсами технологических инноваций в сфере платежей, появились новые угрозы, связанные с кибератаками в финансовом секторе. Преступные методы сегодня становятся более изощренными, с акцентом на сбор и использование конфиденциальной информации, постепенно сводя на нет традиционные механизмы физического хищения средств. Актуальность развития надежных систем для защиты электронных платежей и важных данных требует консолидации усилий со стороны как государства и финансовых организаций, так и общества в целом. Потому в ходе исследования, в целях минимизации цифровых угроз, рассматривается концепция финансовой кибербезопасности, которая способствует устойчивому развитию экономики, а также обеспечению защиты интересов пользователей в условиях постоянно развивающейся цифровой среды.

Ключевые слова: защита данных, инциденты безопасности, денежное обращение, киберугрозы, финансы, экономика.

Реализация товаров, а также нетоварные платежи и расчеты в экономической системе осуществляются посредством денежного обращения. Следует отметить, что роль и сущность денег изменялась в течение многих столетий и продолжает непрерывно эволюционировать. На сегодняшний день, деньги – это универсальное средство обмена, которое используется повсеместно. С их становлением изменился не только быт, но и образ жизни людей, которые смогли совершать более сложные сделки, покупать дорогостоящие товары, услуги, а также хранить свои сбережения. Благодаря совершенствованию технологий и приходу цифровизации произошла трансформация наличных форм денег в безналичные, электронные и переход денежного обращения на электронные платформы, отражая сложность и разнообразие современной финансовой системы. Такой переход обоснован рядом причин, включая изменения в потребительском поведении, удобство проведения сделок, экономические преимущества, осуществление мгновенных, защищенных транзакций. Е. П. Огородникова заключает, что общество вступило в безналичную эпоху, а эпоха наличных денег подходит к концу [1, с. 161]. Поэтому, по мнению Н. И. Кирияковой, основное внимание исследователей современной эры направлено на то, как цифровая трансформация экономики, приводящая к увеличению безналичных расчетов, влияет на систему денежных операций [2, с. 536].

Важно отметить, что наступление цифровой эры и распространение виртуальной формы общения с удаленным партнером или группой, опосредствованное компьютером и системой телекоммуникаций, изменили поведение человека и его отношение к различным средствам платежа.

Социологическое исследование «Отношение населения Российской Федерации к различным средствам платежа», проведенное Банком России в 2023 году, показало, что количество респондентов, которые предпочитают использовать безналичные средства платежа, в 1,8 раза превышает число тех, кто не может не пользоваться наличными деньгами (рис. 1). С 2019 г. по 2023 г. динамика востребованности пользования безналичными средствами непрерывно возрастала, в то время как возможность потребность использовать наличные средства постепенно снижалась[1].

[1] Отношение населения Российской Федерации к различным средствам платежа. Результаты социологического исследования за 2023 год. Результаты социологического исследования за 2023 год. – Банк России, 2024. – 16 с. URL: https://cbr.ru/Collection/Collection/File/49252/results_2023.pdf.

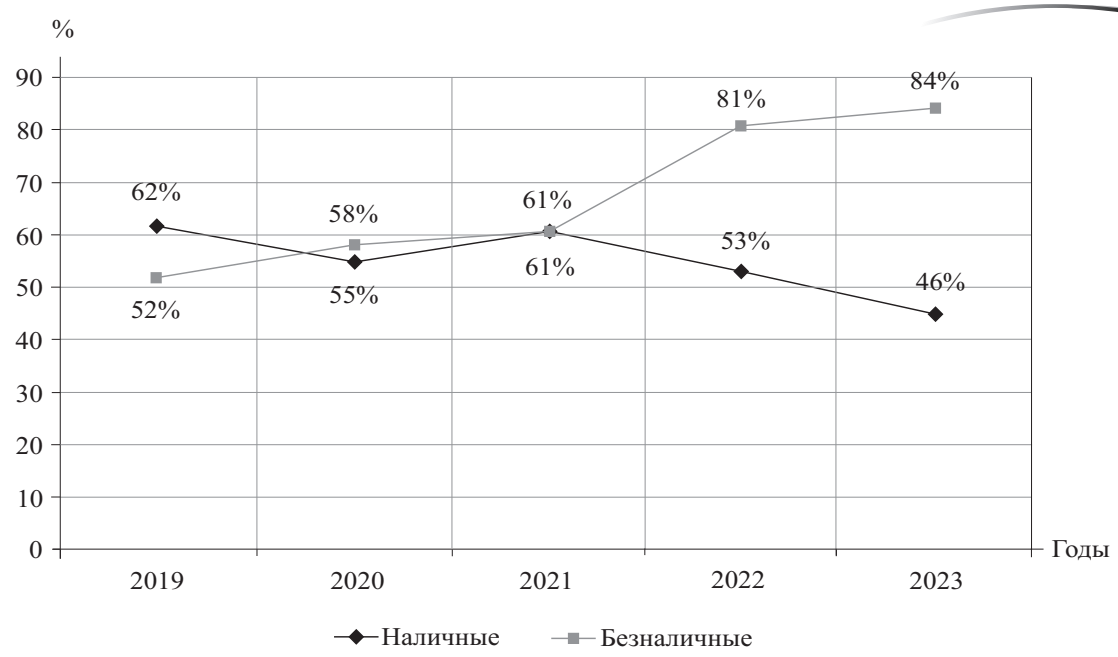

Рис. 1. Распределение ответов респондентов на вопрос об их платежных предпочтениях в период 2019–2023 гг., %

К факторам, влияющим на выбор формы оплаты, опрашиваемые отнесли: наличие необходимого оборудования (смартфона), навыки пользования, время, затрачиваемое на покупку того или иного товара, бонусные программы, скидки, удобство оплаты, удобные точки продаж, а также безопасность и конфиденциальность. Как отмечает А. В. Лисин, у каждого вида платежных инструментов есть свои преимущества и недостатки. Например, наличные расчеты зачастую используются в небольших магазинах, киосках, на рынке, иногда – для оплаты общественного транспорта, автосервиса и др. Безналичный расчет предлагает же дистанционный расчет за приобретаемые товары в интернет-магазинах, мобильную связь, коммунальные услуги, платежи по кредитам, передачу другому лицу денежных средств в кратчайшие сроки, получение заработной платы [3, с. 5]. Поэтому выбор способа расчета зависит от влияния множества составляющих, включая индивидуальные предпочтения и цели каждого отдельного человека.

По мнению участников опроса, к факторам, которые могут стимулировать переход на безналичный контакт, относятся: снижение платы за обслуживания карт и комиссии за переводы, усиление защиты от действий мошенников и интернет-преступников, недопущение раскрытия информации о личном безналичном платеже третьим лицам (рис. 2)[2].

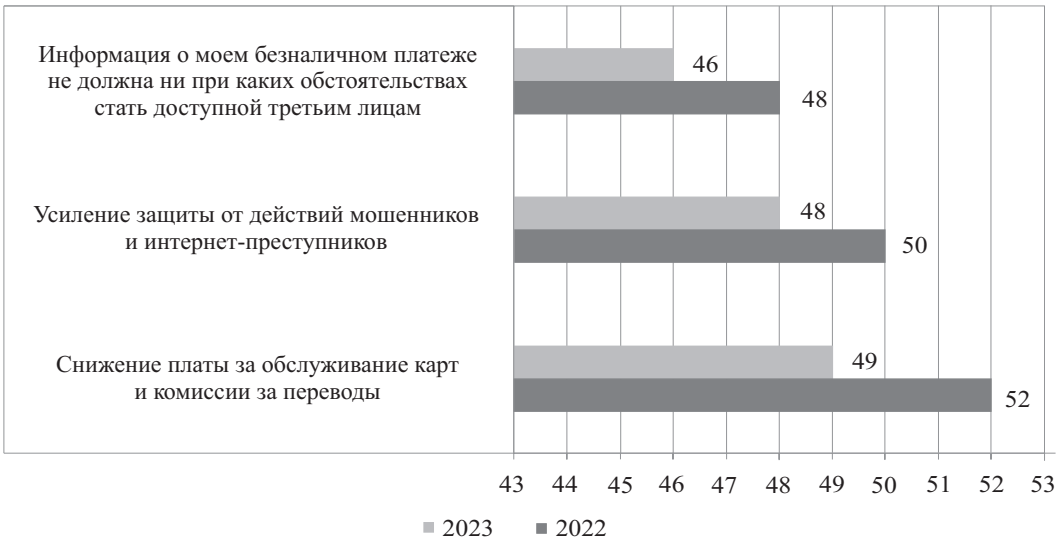

Рис. 2. Распределение ответов респондентов на вопрос о том, что стимулировало бы их использовать безналичные платежные инструменты, %

[2] Там же.

Несомненно, что деньги представляют собой важный элемент современного мира, воздействуют на различные аспекты жизни, оказывая огромное влияние на государство, страну, каждого отдельного человека, определяя тенденции и приводя к изменениям в обществе. Исследования показывают, что деньгам отводится ключевая роль в экономических отношениях, – роль универсального средства определения меры стоимости, средства обращения, сбережения (накопления). Благодаря денежным средствам происходит регулирование рыночных отношений, создание условий для функционирования организаций, стимулирование экономического роста. Кроме того, деньги предоставляют людям шанс расширять свои возможности и свободу выбора, удовлетворять базовые потребности, инвестировать в образование, здоровье, развлечения, развитие бизнеса, а также обеспечивать благосостояние семьи.

Денежные средства стали символом успеха, богатства, превосходства над другими, неуклонно увеличиваясь по значимости с течением времени. Наличие достаточных финансовых средств предоставило их обладателю доступ к различным ресурсам, открыло новые горизонты и укрепило уверенность в своих силах, создавая ощущение превосходства над теми, кто не может себе этого позволить. Зачастую именно успешно зарабатывающие и результативно управляющие своими финансами индивидуумы воспринимаются как более целеустремленные, талантливые, способные. Рост доходов, неравномерное распределение ресурсов усугубляют социальное неравенство, а жадность, корыстные мотивы способствуют коррупции, аморальному поведению. Жажда наживы движет и киберпреступниками.

Активное использование электронных средств и современных форм платежей сопряжено с рядом рисков и киберугроз. Согласно исследованию «Финансовый сектор: Утечки конфиденциальной информации. Мир – Россия 2021–2023», проведенному Экспертно-аналитическим центром InfoWatch, утечка конфиденциальной информации у финансовых организаций в рассматриваемом периоде увеличилась. В 2023 г. было выявлено 1049 таких случаев, что на 79,5 % больше, чем в 2022 г. и почти в 6 раз больше по сравнению с 2021 г. (рис. 3) [4, с. 5].

Увеличение случаев киберпреступности, в том числе хакерских атак, обусловливается развитием технических возможностей, а также усилением внимания к финансовому сектору со стороны преступников. По данным компании Positive Technologies, которая является ведущим разработчиком продуктов и решений, позволяющих выявлять и предотвращать кибератаки, утечки конфиденциальных данных среди последствий атак преобладают и составляют 52 % (рис. 4) [5].

Представленные выше данные свидетельствуют о том, что число более простых и легко реализуемых атак вымогателей и число утечек крупных объемов данных клиентов возросли. Преступники в настоящее время чаще выбирают конфиденциальную информацию как ценный актив, учитывая, что кража денежных средств требует специальных навыков, инструментов. Киберпреступники, находя уязвимые точки в корпоративной инфраструктуре банков и других финансовых организаций, внедряют различные вредоносные программы, взламывают ресурсы через скомпрометированные данные. Информация о платежах и персональных данных клиентов, прежде всего, используется для обмана с применением методов социальной манипуляции, когда человек под психологическим воздействием добровольно переводит денежные средства или раскрывает банковские сведения, позволяющие злоумышленникам совершить хищение, затрудняя их привлечение к ответственности (рис. 5).

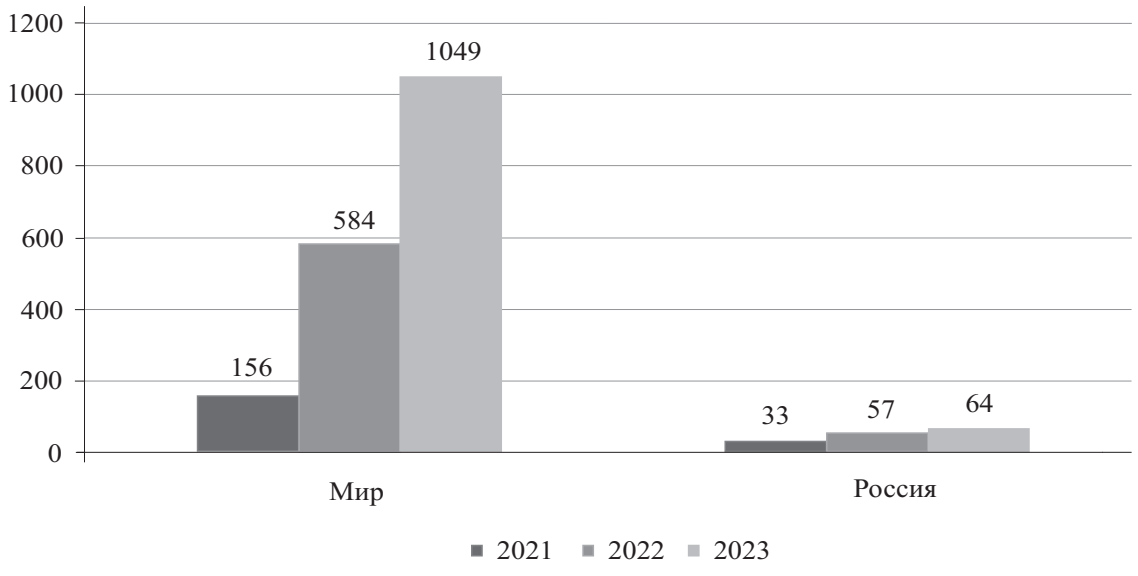

Рис. 3. Количество утечек данных в разделе «Банки и финансовые услуги»

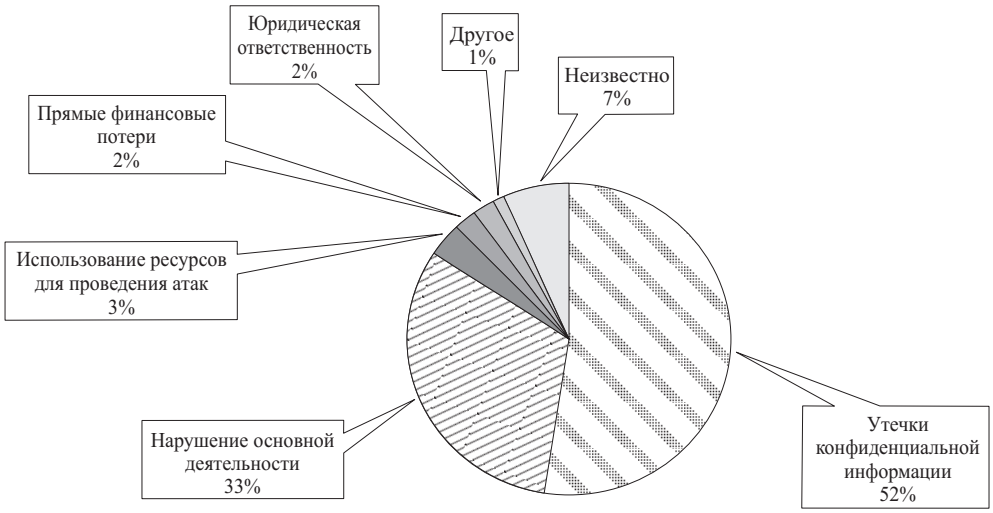

Рис. 4. Результаты последствий успешных атак на финансовые организации

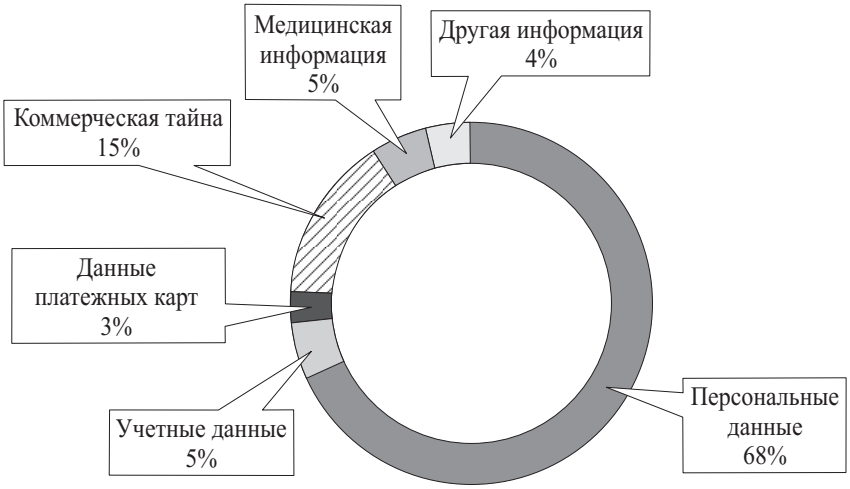

Рис. 5. Типы украденных данных в успешных атаках на финансовый сектор

Ю. В. Ковалева отмечает, что «в рыночных условиях не существует вариантов осуществления банковских операций, в том числе и с пластиковыми картами, которые бы полностью исключали риск и заранее гарантировали определенный финансовый результат. Современный карточный рынок немыслим без риска – риск присутствует в любой операции, он может быть разных масштабов и нейтрализоваться, компенсироваться различными методами» [6, с. 33]. И правда, рыночные условия характеризуются непредсказуемостью спроса и предложения, а также изменениями в экономической ситуации и поведении участников рынка, что делает невозможным определение финансового результата. Ведь вне зависимости от формы обращения денежных средств, пользователи сталкиваются с различными рисками, приводящими к печальным последствиям, материальным и моральным потерям.

Деньги и безопасность взаимосвязаны, особенно в условиях цифрового мира, поскольку угрозы потери или кражи финансовых данных наносят значительный ущерб как частным лицам, так и организациям.

ККиберриски, принимая различные формы, несут серьезную и многогранную угрозу для финансового сектора, начиная от утраты средств клиентов, заканчивая утечками касающейся их конфиденциальной информации, вызывая серьезные проблемы с доверием с их стороны. Если субъекты начинают сомневаться в безопасности своих вложений, то это влечет за собой множественные выводы капитала, что в свою очередь негативно сказывается на репутации и экономическом положении институций. Кроме того, в случае успешно реализованной атаки экономические субъекты несут ответственность за возврат средств клиентам, приводя к банкротству менее устойчивые финансовые организации, в результате чего происходит концентрация капитала в руках нескольких крупных игроков, что снижает уровень конкуренции, сказываясь на развитии отрасли в целом.

Не менее важно отметить, что нарушения надежности, непрерывности предоставления банковских услуг вызывают значительные неудобства и трудности для потребителей. Время, необходимое для восстановления доступа к средствам,

услугам, как правило, варьируется от нескольких часов до нескольких дней, создавая дополнительное напряжение. Зачастую это сводится к прямым убыткам, потере клиентской лояльности. Итогом совокупности этих составляющих является возможность возникновения системного кризиса в банковском секторе. К факторам, способствующим росту угроз, следует также отнести недостаточную защиту данных, низкий уровень финансовой грамотности и финансовой культуры у пользователей банковских услуг и работников кредитных организаций.

Неверное хранение или передача конфиденциальной информации зачастую приводит к утечке данных. Технические сбои в работе банковских систем, цифровых платформ становятся причиной проблем с проведением платежей и доступом к средствам. К счастью, существует множество методов минимизации угроз, способных оказать защиту финансовой сферы.

Одним из направлений информационной безопасности, включающим защиту данных и операций от цифровых угроз, является финансовая кибербезопасность. Это специализированное направление, возникшее в ответ на растущие риски, обусловленные активным использованием электронных платежей, интернет-банкинга, мобильных приложений. Основное его предназначение заключается в защите финансовых систем, данных клиентов, транзакционных процессов от различных атак, мошенничества. Соблюдение мер финансовой кибербезопасности требует применения комплекса технологий, практических подходов, направленных на обеспечение безопасного функционирования финансовых институтов, защиту личной и конфиденциальной информации пользователей, а также предотвращение денежных потерь. Актуальность направления особенно возрастает в условиях дальнейшей цифровизации финансовых услуг, что делает его критически важным элементом общей системы информационной безопасности. Так, финансовая кибербезопасность преследует несколько целей, каждая из которых ориентирована на поддержание стабильности и безопасности:

– соблюдение законодательных и нормативных требований;

– создание и поддержка комплексной системы защиты;

– защита конфиденциальности данных клиентов и организации;

– непрерывность бизнес-процессов и устойчивость к киберугрозам;

– предотвращение мошенничества и других незаконных действий;

– поддержание доверия клиентов.

Достижение целей финансовой кибербезопасности – это долгий непрерывный процесс, так как мир киберугроз и технологий постоянно меняется. Киберпреступники не останавливаются на достигнутом, всегда ищут новые способы взлома систем, а человеческий фактор остается одной из уязвимых точек в области безопасности. Это означает, что финансовые организации должны быть на шаг впереди, постоянно совершенствуя свои защитные меры и стратегии. Любые изменения какой-либо части системы влияют на общую картину защиты, что требует регулярного мониторинга, корректировки. Поэтому для достижения целей финансовой кибербезопасности необходимо следовать ряду конкретных задач, направленных на комплексную защиту. Речь идет, прежде всего, о задачах, которые провозглашены в Основных направлениях развития информационной безопасности кредитно-финансовой сферы на период 2023–2025 годов[3], а именно:

– разработка и внедрение политики безопасности (создании внутренней документации по стандартам безопасности и их соблюдению, контроль выполнения, обновление политики безопасности) – четкие, понятные правила и процедуры обеспечивают согласованность действий и минимизируют риски;

– тестирование и проверка систем безопасности (проведение регулярных тестов на проникновение (пентестов), осуществление аудита безопасности, использование средств для сканирования уязвимостей) – регулярное тестирование позволяет выявить уязвимости до того, как ими воспользуются злоумышленники;

– обучение работников финансовых организаций (периодические тренинги по кибербезопасности, разъяснение политики безопасности, симуляция фишинговых атак) – практика показывает, что именно люди часто являются самым слабым звеном в системе безопасности, поэтому повышение уровня осведомленности работников о киберугрозах и обучение профессиональному поведению помогает предотвратить многие атаки;

– защита данных (шифрование данных, внедрение политики контроля доступа, регулярное обновление и управление паролями, использование многофакторной аутентификации) – защита конфиденциальной информации клиентов и внутренних данных является основополагающим аспектом стратегии кибербезопасности любой организации;

– обнаружение и реагирование на инциденты (создание команды для реагирования на инциденты, внедрение систем мониторинга сети, разработка процедур реагирования на угрозы) – раннее обнаружение атак позволяет смягчить ущерб, быстрая и результативная реакция на потенциальные проблемы критически важна для сохранения целостности и непрерывности бизнеса;

[3] Основные направления развития информационной безопасности кредитно-финансовой сферы на период 2023–2025 годов (одобрены Советом директоров Банка России 22.05.2023). URL: https://cbr.ru/Content/Document/File/148351/onrib_2025.pdf.

– выявление и оценка угроз (проведение аудита безопасности, мониторинг киберугроз, анализ инцидентов, создание базы данных угроз) – для эффективной защиты важно понимать текущие и потенциальные угрозы, регулярный анализ киберугроз позволяет своевременно выявлять новые виды атак и уязвимостей;

– управление рисками (проведение анализа рисков, разработка стратегий управления рисками, внедрение мер по снижению рисков) – как известно, не все риски можно полностью устранить, поэтому важно оценивать и управлять ими, чтобы свести к минимуму возможный ущерб;

– инцидентный ответ и восстановление после атак (разработка и тестирование на практике планов восстановления после атак, обеспечение резервного копирования данных) – даже при высоком уровне защиты, вероятность успешной атаки не исключена, важно иметь план действий на случай инцидента.

Существует множество законов и нормативных актов, регулирующих финансовую кибербезопасность, как на международном уровне, так и в России, позволяющих выстраивать правильную тактику защиты информации [7, с. 4]. Например, наиболее известный международный стандарт ISO/IEC 27001[4] устанавливает универсальные требования для системы управления информационной безопасностью, обеспечивая глобальный подход к защите данных.

В России действуют специализированные законы и нормативные правовые акты, регулирующие вопросы, связанные с обеспечением информационной безопасности, в том числе кибербезопасности. К ним относятся следующие документы:

– Федеральный закон № 152-ФЗ «О персональных данных»[5] и Постановление Правительства РФ «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»[6];

– «Доктрина информационной безопасности Российской Федерации»[7], представляющая собой «систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере» и содержащей такие понятия, как «информационная безопасность Российской Федерации», «обеспечение информационной безопасности», «силы обеспечения информационной безопасности», «средства обеспечения информационной безопасности», «система обеспечения информационной безопасности», «информационная инфраструктура Российской Федерации», а также разделы «Национальные интересы в информационной сфере», «Основные информационные угрозы и состояние информационной безопасности», «Стратегические цели и основные направления обеспечения информационной безопасности», «Организационные основы обеспечения информационной безопасности» [8];

– Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы[8], (далее – Стратегия ИО), определившая «цели, задачи и меры по реализации внутренней и внешней политики Российской Федерации в сфере применения информационных и коммуникационных технологий, направленные на развитие информационного общества, формирование национальной цифровой экономики, обеспечение национальных интересов и реализацию стратегических национальных приоритетов» [8];

– Федеральный закон 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»[9], который был принят сразу после утверждения Стратегии ИО (буквально следом); он был чрезвычайно необходим для реализации «Основных направлений развития информационной безопасности кредитно-финансовой сферы на период 2019–2021 годов»[10], определивших ключевые цели и задачи развития информационной безопасности (ИБ) и киберустойчивости, среди которых следует выделить обеспечение ИБ и киберустойчивости в целях финансовой стабильности каждой организации финансового рынка, обеспечение операционной надежности и непрерывности деятельности организаций кредитно-финансовой сферы, противодействие компьютерным атакам, в том числе при использовании инновационных финансовых технологий,

[4] Международный стандарт ISO/IEC 27001:2022 (Третья редакция 2022-10) «Информационная безопасность, кибербезопасность и защита персональных данных – Системы менеджмента информационной безопасности – Требования» разработан с целью установить требования для создания, внедрения, поддержания функционирования и постоянного улучшения системы менеджмента информационной безопасности (СМИБ), которая обеспечивает сохранение конфиденциальности, целостности и доступности информации за счет выполнения процесса менеджмента риска и дает уверенность заинтересованным сторонам в том, что риски управляются надлежащим образом. Организации должны устанавливать, внедрять, поддерживать функционирование и постоянно улучшать СМИБ, включая необходимые процессы и их взаимодействия, в соответствии с требованиями ISO/IEC 27001:2022.

[5] Федеральный закон от 27 июля 2006 г. № 152-ФЗ (ред. от 08.08.2024) «О персональных данных».

[6] Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

[7] Утв. Указом Президента РФ от 5 декабря 2016 г. № 646.

[8] Утв. Указом Президента РФ от 9 мая 2017 г. № 203.

[9] Федеральный закон от 26 июля 2017 г. № 187-ФЗ (ред. от 10.07.2023) «О безопасности критической информационной инфраструктуры Российской Федерации».

[10] URL: https://cbr.ru/Content/Document/File/83253/onrib_2021.pdf.

защиту прав потребителей финансовых услуг; вышеупомянутые Основные направления развития информационной безопасности кредитно-финансовой сферы на период 2023–2025 годов существенно расширили требования к обеспечению ИБ кредитно-финансовой сферы и способствовали выпуску множества нормативных актов Банка России[11].

Для повышения эффективности функционирования Правительства РФ, ФСБ России, Банка России и других федеральных структур в области обеспечения ИБ Президентом России 1 мая 2022 г. был принят Указ № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации», в который четыре раза вносились изменения и дополнения (Указ действует в ред. от 13.06.2024 г. № 500).

Эти документы предусматривают обязательные меры защиты конфиденциальности, целостности, доступности информации, что помогает финансовым организациям правильно выстроить политику обеспечения кибербезопасности.

Будущее финансовой кибербезопасности обещает радикальные трансформации, вызванные технологическим прогрессом и изменениями в сфере цифровых угроз. В ближайшие годы искусственный интеллект (ИИ), машинное обучение станут ведущими технологиями для мониторинга сетей, анализа данных, что позволит оперативно обнаруживать, предотвращать кибератаки. Внедрение блокчейн-технологий повысит прозрачность и безопасность финансовых транзакций, снижая риск мошенничества. Усиление безопасности идентификации, аутентификации станет критически важным: биометрическая аутентификация с использованием распознавания лиц, отпечатков пальцев усилит защиту, а квантовая криптография обеспечит надежную защиту данных в эру квантовых компьютеров. Ландшафт киберугроз также будет эволюционировать, увеличится количество кибератак с применением искусственного интеллекта, фишинговые атаки станут сложнее, а целенаправленные атаки на финансовую инфраструктуру – более частыми. Автоматизация кибербезопасности станет ключевой тенденцией, так как автоматизированные системы способны быстрее и эффективнее устранять угрозы. Координация усилий между государственными органами, Банком России и частным сектором будет чрезвычайно важна для укрепления финансовой цифровой безопасности.

Таким образом, финансовая кибербезопасность требует не только технологических инноваций, но и стратегического подхода, включающего развитие сотрудничества и постоянное обновление знаний, навыков. Только так можно создать надежную систему защиты, способную противостоять сегодняшним и будущим киберугрозам, обеспечивая безопасность и устойчивое развитие финансовой системы.

Литература

1. *Огородникова Е. П., Лобанова Е. С.* История возникновения денег // Эпоха науки. 2020. № 22. С. 157–162. DOI: 10.24411/2409-3203-2020-12236

2. *Кириякова Н. И.* Соотношение наличных и безналичных в современной экономике: вытеснение или сохранение? // Вестник алтайской академии экономики и права. 2020. № 12 (3). С. 534–539. DOI: 10.17513/vaael.1545

3. *Лисин А. В.* Причины развития безналичного денежного обращения в Российской Федерации // Universum: экономика и юриспруденция. 2022. № 9 (96). С. 4–8.

4. Финансовый сектор: Утечки конфиденциальной информации. Мир – Россия 2021–2023 : Аналитический отчет / Материалы Экспертно-аналитического центра InfoWatch. – М.: InfoWatch, 2023. – 18 с. URL: https://www.infowatch.ru/sites/default/files/analytics/files/finansoviy-sektor-utechki-konfidentsialnoy-informatsii-za-tri-goda-mir-rossiya.pdf.

5. Киберугрозы финансовой отрасли: промежуточные итоги 2023 года. М.: Компания «Positive Technologies»: 2023. – 17 с. URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Financial_industry_security_interim_2023_RU.pdf.

6. *Ковалева Ю. В.* Проблемы рисков в системе электронных денег // Вестник Южно-Уральского государственного университета. Серия: Экономика и менеджмент. 2007. № 10 (82). С. 33–37.

7. Стратегии кибербезопасности: Аналитический отчет / Материалы Экспертно-аналитического центра InfoWatch. – М.: InfoWatch, 2022. – 38 с. URL: https://www.infowatch.ru/sites/default/files/publication_file/analiticheskiy-otchet-strategii-kiberbezopasnosti.pdf.

8. *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.

[11] Положение Банка России от 17 октября 2022 г. № 808-П «О требованиях к обеспечению защиты информации при осуществлении деятельности в сфере оказания профессиональных услуг на финансовом рынке в целях противодействия осуществлению незаконных финансовых операций, обязательных для лиц, оказывающих профессиональные услуги на финансовом рынке, к обеспечению бюро кредитных историй защиты информации, указанной в статье 4 Федерального закона «О кредитных историях», при ее обработке, хранении и передаче сертифицированными средствами защиты, а также к сохранности информации, полученной в процессе деятельности кредитного рейтингового агентства»; Стандарт Банка России «Безопасность финансовых (банковских) операций. Управление инцидентами, связанными с реализацией информационных угроз, и инцидентами операционной надежности. О формах и сроках взаимодействия Банка России с кредитными организациями, некредитными финансовыми организациями и субъектами национальной платежной системы при выявлении инцидентов, связанных с реализацией информационных угроз, и инцидентов операционной надежности» (стандарт СТО БР БФБО-1.5-2023 принят и введен в действие приказом Банка России 8 февраля 2023 г.); Стандарт Банка России «Безопасность финансовых (банковских) операций. Обеспечение безопасности финансовых сервисов с использованием технологии цифровых отпечатков устройств» (стандарт СТО БР БФБО-1.7-2023 введен в действие приказом Банка России от 1 марта 2023 г.) и др.

Сведения об авторах

Следнева Кристина Евгеньевна – студент Омского государственного университета путей сообщения, Омск, Россия.
Email: ksledneva2003@gmail.ru

Кувалдина Татьяна Борисовна – доктор экономических наук, профессор кафедры «Экономическая безопасность и управление финансами», Омский государственный университет путей сообщения, Омск, Россия.
Email: kuvaldina2004@mail.ru

CYBERSECURITY IN THE FINANCIAL SECTOR OF THE ECONOMY: NECESSITY AND SIGNIFICANCE

K. Sledneva, T. Kuvaldina
Omsk State Transport University,
Omsk, Russia

In the age of technological development, the financial sector of the Russian economy was one of the first to actively begin the transition to digitalization of all business processes. Electronic platforms have been used to accelerate financial transactions and improve the quality of financial services. The country's population is increasingly moving towards cashless payments for goods, works and services. Russians now have the opportunity to purchase digital assets via bank card on a variety of electronic resources without leaving home. Nevertheless, along with the pluses of technological innovations in the payments sphere, new threats related to cyberattacks in the financial sector have emerged. Criminal methods today are becoming more sophisticated, with an emphasis on the collection and use of confidential information, gradually nullifying the traditional mechanisms of physical theft of funds. The urgency of developing reliable systems to protect electronic payments and important data requires the consolidation of efforts on the part of both the state and financial organizations, as well as society as a whole. Therefore, in the course of the study, in order to minimize digital threats, the concept of financial cybersecurity is considered, which contributes to the sustainable development of the economy, as well as ensuring the protection of users' interests, in a constantly evolving digital environment.

Keywords: data protection, security incidents, money circulation, cyber threats, finance, economics.

References

1. Ogorodnikova E. P., Lobanova E. S. The history of money, *Epokha nauki*, 2020, No. 22, pp. 157-162 (In Russ.). DOI: 10.24411/2409-3203-2020-12236

2. Kiriyakova N. I. The ratio of cash and non-cash in the modern economy: displacement or preservation? *Vestnik altaiskoi akademii ekonomiki i prava*, 2020, No. 12 (3), pp. 534-539 (In Russ.). DOI: 10.17513/vaael.1545

3. Lisin A. V. The reasons for the development of non-cash money circulation in the Russian Federation, *Universum: ekonomika i yurisprudentsiya*, 2022, No. 9 (96), pp. 4–8. (In Russ.).

4. *Finansovyj sektor: utechki konfidencial'noj informacii (Mir – Rossija, 2021-2023)* [Financial sector: leaks of confidential information (Mir – Russia, 2021–2023)]. Moscow: InfoWatch, 2023, 18 p. (In Russ.). Available at: https://www.infowatch.ru/sites/default/files/analytics/files/finansoviy-sektor-utechki-konfidentsialnoy-informatsii-za-tri-goda-mir-rossiya.pdf (accessed 15 July 2024).

5. *Kiberugrozy finansovoj otrasli: promezhutochnye itogi 2023 goda* [Cyber threats to the financial industry: interim results of 2023], Moscow: Kompaniya “Positive Technologies”, 2023, 17 p. (In Russ.). Available at: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Financial_industry_security_interim_2023_RU.pdf (accessed 15 July 2024).

6. Kovaleva Yu. V. Problems of risks in the electronic money system, *Vestnik Yuzhno-Ural'skogo gosudarstvennogo universiteta. Seriya: Ekonomika i menedzhment*, 2007, No. 10 (82), pp. 33–37. (In Russ.).

7. *Analiticheskij otchet strategii kiberbezopasnosti* [Cybersecurity Strategy Analytical Report], Moscow: InfoWatch, 2022, 38 p. (In Russ.). Available at: https://www.infowatch.ru/sites/default/files/publication_file/analiticheskiy-otchet-strategii-kiberbezopasnosti.pdf (accessed 15 July 2024).

8. 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. DOI: https://doi.org/10.34020/1993-4386-2024-2-50-60

About the authors

Kristina E. Sledneva – student of Omsk State Transport University (OSTU), Omsk, Russia.
Email: ksledneva2003@gmail.ru

Tatyana B. Kuvaldina – Doctor of Economics, Professor of the Department of Economic Security and Financial Management, Omsk State Transport University (OSTU), Omsk, Russia.
Email: kuvaldina2004@mail.ru