Киберпреступность и кибермошенничество на финансовом рынке

Bercrime and Cyberfraud in the Financial Market

DOI: 10.12737/2306-627X-2025-14-1-49-56 Получено: 08 февраля 2025 г. / Одобрено: 19 февраля 2025 г. / Опубликовано: 31 марта 2025 г.

Асяева Э.А.

Канд. экон. наук, доцент кафедры мировых финансовых рынков и финтеха, ФГБОУ ВО «Российский экономический университет им. Г.В. Плеханова», г. Москва,
e-mail: asyaeva.ea@rea.ru

Мягкова Ю.Ю.

Канд. экон. наук, доцент, доцент кафедры мировых финансовых рынков и финтеха, ФГБОУ ВО «Российский экономический университет им. Г. В. Плеханова», г. Москва,
e-mail: myagkova.yy@rea.ru

Asyaeva E.A.

Candidate of Economic Sciences, Associate Professor, Department of Global Financial Markets and Fintech, Plekhanov Russian University of Economics, Moscow,
e-mail: asyaeva.ea@rea.ru

Myagkova Yu.Yu.

Candidate of Economic Sciences, Associate Professor, Department of Global Financial Markets and Fintech, Plekhanov Russian University of Economics, Moscow,
e-mail: myagkova.yy@rea.ru

Аннотация

В статье рассматриваются актуальные проблемы киберпреступности и кибермошенничества на современном финансовом рынке. Исследуются основные виды и методы совершения киберпреступлений в финансовой сфере. Представлен анализ рисков киберпреступлений электронного банкинга, выявлены факторы, влияющие на динамику распространения киберпреступности. Рассматриваются причины повышения количества утечек данных и кибератак на российском финансовом рынке, а также даны рекомендации по обеспечению кибербезопасности финансовых институтов и учреждений.

Ключевые слова: киберпреступность, кибермошенничество, финансовый рынок, информационная безопасность, цифровые технологии, цифровизация.

Abstract

The article examines the current problems of cybercrime and cyberfraud in the modern financial market. The main types and methods of committing cybercrimes in the financial sector are studied. An analysis of the risks of cybercrimes in electronic banking is presented, factors influencing the dynamics of the spread of cybercrime are identified. The reasons for the increase in the number of data leaks and cyberattacks in the Russian financial market are considered, and recommendations are given for ensuring the cybersecurity of financial institutions and agencies.

Keywords: cybercrime, cyberfraud, financial market, information security, digital technologies, digitalization.

ВВЕДЕНИЕ

Актуальность темы обусловлена тем, что цифровизация стала глобальным, всеобъемлющим процессом, затрагивающим все стороны общественной жизни. Финансовый рынок претерпевает системные трансформации, интегрируя свои сегменты и институты в глобальное цифровое пространство. Такая интеграция превращает их в компоненты глобальной информационной системы и устанавливает различную степень зависимости от нее.

Современная практика показывает, что глобальное развитие, обусловленное цифровизацией, создает новые вызовы, угрозы и риски для информационной безопасности. Проблемы информационной безопасности, защиты компьютерных данных, защиты конфиденциальной информации, засекреченной законом, и подобные вопросы имеют особую значимость как для Российской Федерации, так и во всем мире. В настоящее время финансовый рынок несет на себе основную тяжесть потерь, связанных с киберпреступностью, учитывая его значение как центра аккумулирования денежных средств домашних хозяйств и предприятий.

Банк России определил появление новых видов мошенничества и киберпреступности как ключевую проблему в развитии финансового рынка. В рамках Стратегии повышения финансовой грамотности и культуры к 2030 г. также подчеркивается необходимость обеспечения финансовой кибербезопасности.

Следовательно, все аспекты развития киберпреступности напрямую связаны со стремлением к незаконному завладению финансовыми ресурсами. Важно отметить, что данная тема и дальше будет оставаться актуальной, поскольку прогресс в технических и юридических мерах защиты приводит к соответствующему совершенствованию тактики киберпреступников.

МЕТОДЫ ИССЛЕДОВАНИЯ

Методологическая база исследования основывается на использовании диалектического метода изучения социальных процессов и явлений. Использованы такие методы, как сравнительно-исторический, метод системного анализа, статистического анализа, систематизации, обобщения.

Информационную базу исследования составили статистическая отчетность по киберпреступности и кибермошенничеству на российском финансовом рынке, нормативно-правовые акты по предотвращению распространения киберпреступности, публикации, научные публикации по тематике исследования.

РЕЗУЛЬТАТЫ

Принято разграничивать понятия мошенничества и финансовых преступлений, однако различия между ними становятся всё менее четкими из-за роста числа киберугроз, усложнения преступных схем и усиления взаимосвязей между различными видами преступлений. Также к числу проблем можно отнести отсутствие законодательного разделения этих понятий, разное толкование их регулирующими органами и организационную разобщенность в подходах к классификации.

Такая ситуация требует пересмотра традиционных подходов к категоризации финансовых преступлений и разработки более современных методов их выявления и предотвращения.

Под мошенничеством понимаются такие преступления, как подделка документов, кредитное мошенничество, инсайдерские угрозы, включающие обман персонала с целью совершения кражи. Финансовые учреждения, как правило, рассматривают мошенничество как источник убытков.

В связи со стиранием границ между различными видами финансовых преступлений, банки и другие финансовые учреждения вынуждены применять единый комплекс инструментов для защиты от всех типов угроз, будь то мошенничество или киберпреступления.

Под термином «киберпреступность» следует понимать вид преступления, совершенные с помощью компьютерной техники, смартфона и других специальных технических средств, что приводит к мошенничеству в сети, использованию нелицензионных программ и других видов преступлений [8].

Как отмечает А.Н. Харитонов, киберпреступление является одной из величайших проблем современности, с которой вынужденно столкнулось человечество, несмотря на то, в какой стране произошло преступление. Такое положение вещей будет постоянно обостряться, поскольку технологический процесс не стоит на месте [1]. Стоит отметить, что развитие технологического прогресса происходит гораздо быстрее развития нормативно-правовой базы относительно преступлений в киберпространстве.

Как утверждает Т.А. Далгалы, понятие киберпреступность употребляется наряду с термином «компьютерная преступность». Эти два понятия тождественны, но киберпреступность значительно шире, поскольку охватывает не только цифровое пространство, но и телекоммуникационные сети и в целом все информационное пространство [3].

К.Н. Евдокимов считает, что киберпреступность – это противоправные действия, совершаемые лицами, в целях умышленного преступления, с использованием компьютерных технологий, для похищения материальных или интеллектуальных ценностей [4].

Проанализировав теоретические и практические исследования в области определения понятия киберпреступности, можно прийти к заключению, что на данном этапе развития не существует единого подхода к определению понятия киберпреступности. Более того, подходы существенно отличаются, что может привести к недоразумениям и, в свою очередь, к неправильной идентификации преступных деяний, что проблематично не только с теоретической, но и с практической точки зрения.

Киберпреступление и кибермошенничество — это близкие, но не идентичные понятия.

Киберпреступление — это более широкий термин, который охватывает любой вид преступной деятельности, совершаемый с использованием компьютерных технологий. Кибермошенничество — это более узкое понятие, которое относится к преступной деятельности, направленной на обман или кражу денег у людей с использованием компьютерных технологий. Кибермошенничество — это подтип киберпреступления. Все кибермошенничество является киберпреступлением, но не все киберпреступления являются кибермошенничеством.

В рейтинге экономических преступлений киберпреступления занимают пятую позицию, уступая таким видам противоправной деятельности, как незаконное присвоение активов, коррупционные схемы и взяточничество, нарушение принципов честной конкуренции, а также фальсификация финансовых документов (рис. 1).

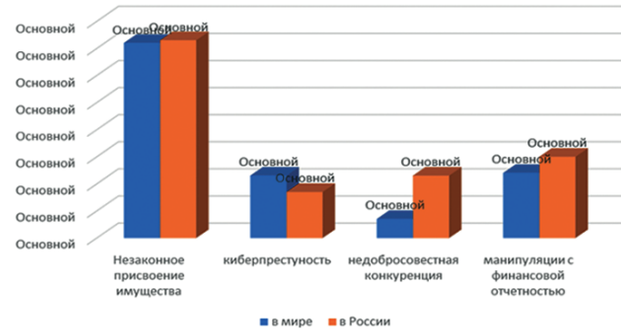

Рис. 1. Самые распространенные экономические преступления в России и в мире
Источник: составлено авторами на основе данных [7].

Главным объектом мошенничества являются ресурсы банковских учреждений. Кроме того, компьютерных атак на банковскую систему намного больше, чем свидетельствует официальная статистика. Это объясняется тем, что многие кибератаки являются не-

удачными, а обнаруженные пробелы в системе электронного банкинга быстро восстанавливаются [5].

Основные виды киберпреступлений, совершаемых в банковской деятельности, обобщены в табл. 1.

Таблица 1

Виды киберпреступлений в финансовой сфере

Название	Характеристики
Мошенничество с пластиковыми картами	Получение доступа к банковским картам клиентов с целью списания денежных средств
Фишинг	Злоумышленники отправляют фальшивые электронные письма или SMS, под видом официального запроса от банка или финансовой организации, с целью получения личной информации пользователей
Кибератаки на банковский сектор	Попытки проникновения в системы банков или финансовых учреждений, чтобы получить доступ к конфиденциальным данным, украсть средства или просто нарушить работу системы
Криптовалютные мошенничества	Кража криптовалют, мошеннические схемы ICO (Initial Coin Offering) или пирамидальные схемы с криптовалютами
Экологические атаки	Злоумышленники могут использовать вредоносное ПО для заражения компьютеров и сетей финансовых организаций с целью шантажа или выполнения угроз
Пеймент-криминал	Использование преступниками процессинговых и иных платежных систем
Программный инжиниринг	Представляет собой сочетание хакерства со злонамеренным внесением в программный код покупных или собственных программ, ответственных за хранение, учет, обработку данных, и принятие на их основе финансовых и инвестиционных решений

Источник: составлено авторами на основе данных [13].

Киберпреступники постоянно совершенствуют свои методы, поэтому финансовым учреждениям необходимо непрерывно обновлять системы защиты и повышать осведомленность пользователей.

Следует отметить, что риск информационной безопасности (включая киберриск) и риск информационных систем являются частью операционного риска [11].

Сегодня основными источниками риска киберпреступлений в условиях электронного банкинга являются операции, связанные с платежными картами, обслуживание через банкоматы, обслуживание в системе Интернет-банкинга, а также использование мобильных приложений для обслуживания через систему мобильного банкинга. Поэтому для качественной идентификации риска киберпреступлений электронного банкинга его следует разделять на:

1) риск мошенничества с платежными карточками;
2) риск мошенничества с банкоматами;
3) риск мошенничества с мобильным телефоном и Интернетом (рис. 2).

Рис. 2. Классификация киберпреступлений в условиях электронного банкинга

Источник: составлено автором на основе данных [2].

Существенное увеличение количества зарегистрированных с 2020–2023 гг. киберпреступлений некоторые ученые связывают с ежегодным ростом пользователей [12].

Помимо роста интернет-пользователей, на динамику распространения киберпреступности влияют следующие факторы:

- стремительное развертывание процесса информатизации общества (внедрение сети третьего поколения (5G) операторами мобильной связи;
- осваивание кибертехнологий как средства преступной деятельности, объективное отставание технической составляющей правоохранительной системы и т.д.

Географическое распределение преступности также имеет значение. Именно техническое (соответственно, и финансовое) развитие невозможно себе представить без привлечения современных информационных технологий. При этом анализ географических особенностей отдельных видов киберпреступлений позволил выявить специфику. Некоторые преступления имеют традиционную «принадлежность» к месту совершения. Это такие преступления, как создание с целью использования, распространения или сбыта вредоносных программ или технических средств, а также их распространение или сбыт; несанкционированный сбыт или распространение информации с ограниченным доступом, хранящейся в ЭВМ (компьютерах), автоматизированных системах, компьютерных сетях или на носителях такой информации и нарушение правил эксплуатации автоматизированных ЭВМ (компьютеров), автоматизированных систем, компьютерных сетей или сетей электросвязи или порядка или правил защиты обрабатываемой в них информации.

Рынок финансовых услуг претерпел значительные изменения под влиянием бурного развития цифровых технологий, что создало серьезные вызовы для дальнейшего существования классических финан-

совых организаций. Исследования показывают, что стремительное внедрение инновационных решений может привести к потере финансовыми компаниями до одной трети их доходов [10]. В сложившейся ситуации финансовые организации всё чаще вступают в партнерские отношения с финтех-компаниями и существенно увеличивают инвестиции в обновление своей инфраструктуры, совершенствование операционных процессов, улучшение клиентского сервиса и укрепление систем информационной защиты. Обеспечение кибербезопасности – основная задача финансовых учреждений и национальных финансовых регуляторов. На сегодняшний день противодействие киберугрозам является одной из главных тем для обсуждения на международных экономических форумах и конференциях, данная проблематика широко освещена в трудах зарубежных ученых.

Экономическая безопасность любого государства находится под серьезной угрозой из-за кибермошенничества и отмывания незаконно полученных средств. Данная проблема приобретает всемирный масштаб, поскольку многочисленные механизмы легализации преступных доходов выходят за пределы национальных границ и тесно переплетаются с деятельностью транснациональных преступных синдикатов.

В 2023 г. специалистами было зафиксировало 6,8 тыс. киберинцидентов в кредитно-финансовом секторе, что составляет пятую часть от общего числа выявленных инцидентов информационной безопасности. При этом за последние два года количество ИБ (информационная безопасность) — событий в банковской сфере увеличилось на 75%, что немного ниже средних показателей в других отраслях (где рост составил 90%) [10].

В течение 2022 г. кибератаки преимущественно носили массовый характер. Направленные атаки встречались реже из-за необходимости серьезных ресурсов и специальных навыков злоумышленников. В настоящее время организации стараются расширить охват систем мониторинга информационной безопасности, однако сталкиваются с техническими ограничениями традиционных *SIEM*-решений. В связи с этим, на фоне растущей сложности кибератак, всё большее значение приобретают специализированные решения такие, как *NTA* (*Network Traffic Analysis*), *EDR* (*Endpoint Detection and Response*) и др.

В финансовом секторе за 2023 г. зафиксировано следующее распределение киберинцидентов по уровню критичности:

1) средняя критичность — 61% (преобладающая часть);
2) низкая критичность — 38% (чуть более трети);
3) высокая критичность — 1% (единичные случаи).

Такая статистика указывает на два ключевых тренда: во-первых, злоумышленники стали действовать более продуманно и методично, во-вторых, наблюдается тенденция к усложнению техник проведения кибератак.

Преобладание инцидентов средней критичности (более половины всех случаев) свидетельствует о серьезном уровне подготовки и стремлении проводить многоэтапные операции, избегая при этом немедленного обнаружения, которое характерно для атак высокой критичности.

В частности, киберразведка и первичное проникновение в инфраструктуру становятся предшественниками киберударов, возможно с участием внутреннего нарушителя. Этому способствует также большое количество утечек данных, произошедших за последние полтора года, что привело к раскрытию информации, включая данные о корпоративных аккаунтах.

За 2023 г. в финансовой сфере наблюдалось ухудшение ситуации с кибербезопасностью. Количество случаев утечек конфиденциальных данных выросло на 12,3%, а кибератак увеличилось более чем на четверть [15]. Согласно исследованию экспертно-аналитического центра ГК *InfoWatch*, количество утечек конфиденциальных данных из финансовых компаний продолжает расти быстрыми темпами [14]. Глобально этот индикатор вырос на 79,5%, достигнув рекордного показателя в 1049 случаев.

Рост числа киберинцидентов в России также оказался достаточно высоким и в 2023 г. достиг 12,3% (64 случая). Объем утекшей из финансовой отрасли информации увеличился в разы. Например, если по всему миру в 2023 г. из организаций было украдено 4324 млн записей персональных данных (в шесть раз больше, чем годом ранее), то в России за тот же период — 170,3 млн (в 3,2 раза больше, чем в 2022 г.). Для сравнения в 2021 г. этот показатель в России составил 3 млн записей, что почти в 57 раз меньше, чем в 2023 г.

Одним из главных факторов, которые привели к значительному увеличению числа утечек в сфере аналитики — это быстрый темп цифровизации финансового сектора и обнаружение новых уязвимостей. Присутствие этих новых уязвимостей приводит к увеличению числа взломов компаний и расширению объема скомпрометированной информации. На фоне этой динамики большинство компаний не спешат раскрывать информацию об инцидентах. Согласно исследованию ГК *InfoWatch*, 42% представителей финансовой отрасли считают, что только от 4 до 10% компаний признают факт утечки данных.

Структура утечек по типам данных представлена на рис. 3.

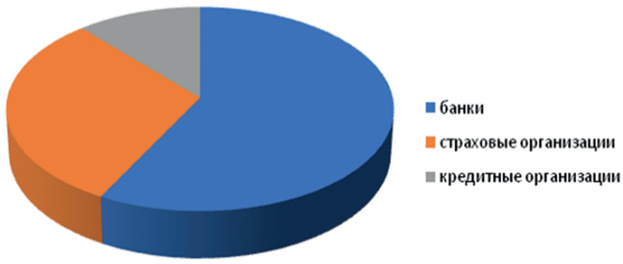

Рис. 3. Распределение организаций на финансовом рынке по объемам утечки информации, %

Источник: составлено авторами на основе данных [9].

Согласно структуре утечки информации по типам организаций финансового сектора в России, наибольшую долю занимают банки — в 2023 г. это было 46,9%. На втором месте оказались страховые организации, доля которых в прошлом году выросла до 25%, а на третьем месте — кредитные организации с результатом в 9,4%.

Виды утечек данных из финансовых учреждений представлены на рис. 4.

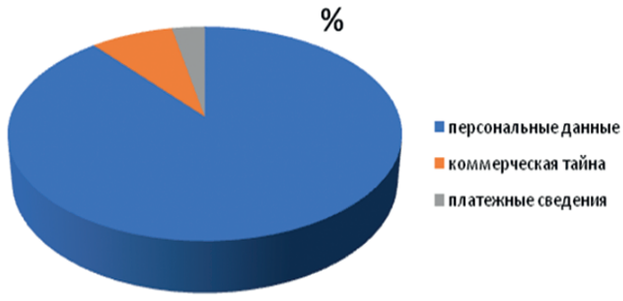

Рис. 4. Виды утечек информации, %

Источник: составлено авторами на основе данных [6].

В России наибольшую долю утекшей информации из финансовых компаний в 2023 г. составляют персональные данные — 87,5%. Однако наблюдается некоторое снижение этой доли. Далее идут данные, содержащие коммерческую тайну (7,8%) и платежные сведения (3,1%).

Среди других тенденций аналитики отмечают рост умышленной утечки информации, доля которой в России за последние три года достигла 87,5%. Аналитики считают, что значительная часть кибератак может иметь гибридный характер или служить прикрытием для внутренних хищений.

По материалам статистических данных Российская Федерация занимает второе место среди стран с долей в 6,1% утечек в финансовом секторе. Лидером являются США с долей в 44,3%.

Часть атак связана с эксплуатацией уязвимостей (36%), несанкционированным доступом к системам и сервисам (28%) и сетевыми атаками (14%) (рис. 5).

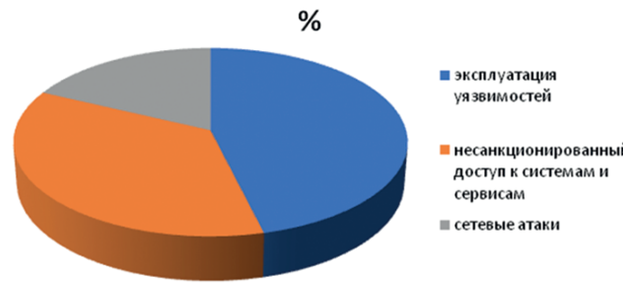

Рис. 5. Направления кибепреступлений в финансовом секторе Российской Федерации

Источник: составлено авторами на основе данных [9].

Каждый третий инцидент в банковском секторе обусловлен эксплуатацией уязвимых мест в системах защиты. Киберпреступники используют эти уязвимости на различных стадиях своих атак. Изначально происходит компрометация веб-ресурсов, проникновение в программные приложения и нападение на внешние сервисы, после чего злоумышленники переходят к дальнейшим этапам — распространению внутри корпоративной сети, эскалации привилегий и, в конечном итоге, получению доступа к критически важным банковским системам. Растет количество случаев несанкционированного доступа к АБС (автоматизированные банковские системы), ДБО (дистанционное банковское обслуживание), системам внутреннего документооборота и ключевым базам данных. Поэтому для защиты банковской инфраструктуры критически важны своевременное обновление ПО (патч-менеджмент), эффективное управление уязвимостями, постоянный мониторинг безопасности, контроль доступа к критическим системам. Эти меры являются базовым уровнем защиты банковской инфраструктуры от современных киберугроз.

Интересно, что всего лишь 4% всех инцидентов в банковской сфере связаны с заражением вредоносным ПО, что говорит о высоком уровне зрелости финансовых учреждений, которые обеспечивают высокий уровень базовой защиты информационно-технологической инфраструктуры, включая антивирусную защиту и соблюдение политики информационной безопасности сотрудниками. Именно эти меры чаще всего приводят к обнаружению инцидентов.

Банки заранее создали устойчивые системы безопасности до резкого увеличения киберугроз, и сейчас основное внимание уделяется обновлению и

внедрению совершенно новых решений. Несмотря на то что расходы на информационную безопасность финансовых организаций в 2023 г. составили 20 млрд руб., что превышает бюджеты федеральных органов исполнительной власти, отрасль сталкивается с проблемой недостаточного финансирования. За год бюджеты на информационную безопасность выросли на 5%, в то время как рост ИТ-бюджетов в финансовом секторе составил 12%, достигнув 343 млрд руб. в 2023 г. По прогнозам специалистов из «Солар», финансовые компании будут увеличивать степень защиты информации, и к 2030 г. их расходы в этой области могут достичь 30 млрд руб. Несмотря на увеличение этих расходов, эксперты считают, что финансовые компании нуждаются в дополнительном финансировании для укрепления кибербезопасности. Это позволяет сделать следующий вывод: в число успешных борцов с кибертеррористами вошли финансовые организации, имеющие опыт противодействия атакам или выработавшие собственную бизнес-практику кибербезопасности.

ОБСУЖДЕНИЕ И ЗАКЛЮЧЕНИЕ

Киберпреступность и кибермошенничество представляют собой значительную и постоянно развивающуюся угрозу для финансового рынка. Разнообразие тактик, используемых киберпреступниками, в сочетании с растущей зависимостью от цифровых технологий, требует многогранного подхода к борьбе с этими угрозами.

Повышение количества утечек данных и кибератак в российском финансовом секторе может быть обусловлено несколькими причинами.

1. Финансовые учреждения хранят значительное количество конфиденциальной информации, включая данные клиентов, что делает их привлекательной целью для киберпреступников.
2. С развитием новых технологий и цифровизацией банковских услуг расширяются возможности для осуществления атак и появляются новые уязвимости, которые могут быть использованы злоумышленниками.
3. Некоторые финансовые учреждения могут обладать недостаточной защитой данных, использовать устаревшее программное обеспечение или иметь недостаточно подготовленный персонал, что делает их уязвимыми перед угрозами в области кибербезопасности.

Таким образом, сегодня существует объективная необходимость усиления мероприятий по обеспечению безопасности финансовых институтов и учреждений.

Наиболее распространенным видом киберпреступлений в банковских учреждениях стали атаки на счета клиентов. Злоумышленники постоянно совершенствуют способы получения доступа к банковским аккаунтам, перехвата платежной информации, хищения финансовых средств, обхода систем защиты банков.

В современных условиях необходимо использовать комплекс программных и технических средств, который бы обеспечивал высокий уровень защиты инфраструктуры при сохранении достаточной эффективности технологических процессов. Для предотвращения атак эффективны методы социальной инженерии – регулярное инструктирование всех сотрудников компании о безопасной работе в Интернете и информирование их о существующих видах угроз.

Сегодня основной задачей Российской Федерации в сфере финансовой безопасности является достижение стратегической автономии, которая предоставит возможность быть независимой от разработок иностранных программ.

Развитие цифровой экономики и промышленности 4.0 характеризуется слиянием различных областей знаний, промышленных секторов и социальных сфер в единую взаимосвязанную систему. Этот процесс выходит за рамки внедрения отдельных технологий, формируя глобальную сеть взаимодействий, которая вызывает фундаментальные структурные изменения во всех странах, отраслях и обществе в целом.

Возрастание связи и зависимости от цифровых услуг и ключевых компонентов для развития цифровых технологий, которые считаются критическими. Примером является производство полупроводников и микросхем для обеспечения базовых потребностей цифровизации, являющихся частью глобальных цепей добавленной стоимости и включает высокую степень разделения труда, значительные капиталовложения, специальные знания и длительное время производства.

Финансовый рынок Российской Федерации на современном этапе развивается в условиях полномасштабной перестройки, поскольку санкции привели к внутренним изменениям финансовых услуг и учреждений.

Укрепление партнерских связей в области кибербезопасности и совместный обмен информацией о киберугрозах играют ключевую роль в уменьшении риска кибератак. Сотрудничество и создание отраслевых альянсов позволяют компаниям коллективно повысить свою защищенность. Использование искусственного интеллекта, особенно нейронных

сетей, помогает справиться с усложняющимися угрозами быстро и эффективно, обрабатывая большие объемы данных в реальном времени и адаптируясь к новым угрозам на 98% быстрее, чем стандартные методы.

В свете текущей неопределенности и широкомасштабной перестройки экономической системы страны финансовый рынок стоит перед задачей разработки стратегии нацеленной на импортозамещение, привлечение высококвалифицированных специалистов и обучение новых кадров для обеспечения кибербезопасности. Важным аспектом является постоянный мониторинг киберрисков и выработка мер по их нейтрализации.

Масштабная перестройка финансового рынка в условиях санкций и усиливающихся кибератак, требует стратегического планирования с учетом цифрового перехода, который включает разработку стратегических документов и дорожных карт по цифровому развитию. Однако для достижения цифровой автономии необходимо решить проблемы, вызванные обеспечением доступа к интернету, развитием ИТ услуг, цифровых навыков, научно-технических разработок и инновационной инфраструктуры.

Литература

1. *Алоева А.А.* Информационный терроризм угроза национальной безопасности в условиях цифровизации [Текст] / А.А. Алоева, И.А. Алоев, А.З. Жуков // Пробелы в российском законодательстве. — 2020. — Т. 13. — № 6. — С. 197–201.
2. *Батурин Ю.М.* Что делает виртуальные преступления реальными [Текст] / Ю.М. Батурин, С.В. Полубинская // Труды Института государства и права Российской академии наук. — 2021. — Т. 13. — № 2. — С. 9–11.
3. *Далгалы Т.А.* Киберкриминология: вызовы XXI века // Рос. юстиция. — 2020. — № 10. — С. 19.
4. *Евдокимов К.Н.* Вредоносные компьютерные программы как орудие и средство совершения преступлений: онтологические и гносеологические аспекты [Текст] / К.Н. Евдокимов // Рос. юстиция. — 2020. — № 3. — С. 56–61.
5. *Иванова Л.В.* Виды киберпреступлений по российскому уголовному законодательству [Текст] / Л.В. Иванова // Юридические исследования. — 2019. — № 1. — С. 25–31.
6. Киберпреступления в России: тенденции 2023 года [Электронный ресурс]. — URL: https://cloudnetworks.ru/analitika/kiberprestupleniya-v-rossii-tendentsii-2023-goda (дата обращения: 20.02.2025).
7. Крупнейшие компании России в сфере защиты информации. Обзор CNews Security: Информационная безопасность // Рейтинг сетевого издания CNews [Электронный ресурс]. — URL: https://www.cnews.ru/reviews/security_2023/articles/sanktsii_vdohnuli_novuyu_zhizn_v_rossijskij (дата обращения: 23.02.2025).
8. *Кули-Заде Т.А.* Проблемы квалификации мошенничества в сфере компьютерной информации [Текст] / Т.А. Кули-Заде // Рос. юстиция. — 2019. — № 4. — С. 21.
9. Официальный сайт Росстат [Электронный ресурс]. — URL: https://rosstat.gov.ru (дата обращения: 14.02.2025).
10. Официальный сайт Федеральной налоговой службы [Электронный ресурс] URL: https://www.nalog.gov.ru/rn77 (дата обращения: 14.02.2025).
11. Положения Банка России от 8 апреля 2020 года № 716-П «О требованиях к системе управления операционным риском в кредитной организации и банковской группе», зарегистрированного Министерством юстиции Российской Федерации 3 июня 2020 года № 58577 (далее — Положение Банка России № 716-П).
12. *Семеко Г.В.* Информационная безопасность в финансовом секторе: киберпреступность и стратегия противодействия // Социальные новации и социальные науки. — 2020. — № 1. — С. 77–79.

References

1. Aloeva A.A., Aloev I.A., Zhukov A.Z. Information terrorism is a threat to national security in the context of digitalization // Gaps in Russian legislation. 2020, vol. 13, no. 6, pp. 197–201.
2. Baturin Yu.M., Polubinskaya S.V. What makes virtual crimes real // Proceedings of the Institute of State and Law of the Russian Academy of Sciences. 2021, vol. 13, no. 2, pp. 9–11.
3. Dalgaly T.A. Cybercriminology: challenges of the XXI century // Russian Justice. 2020, no. 10, p. 19.
4. Evdokimov K.N. Malicious computer programs as a tool and means of committing crimes: ontological and epistemological aspects // Russian Justice. 2020, no. 3, pp. 56–61.
5. Ivanova L.V. Types of cybercrimes under Russian criminal law // Legal research. 2019, no. 1, pp. 25–31.
6. Cybercrimes in Russia: trends in 2023 [Electronic resource] URL: https://cloudnetworks.ru/analitika/kiberprestupleniya-v-rossii-tendentsii-2023-goda (accessed 02/20/2025).
7. Russia's largest companies in the field of information security. Review of CNews Security: Information Security // Rating of the Cnews online publication [Electronic resource] URL: https://www.cnews.ru/reviews/security_2023/articles/sanktsii_vdohnuli_novuyu_zhizn_v_rossijskij (accessed 02/23/2025).
8. Kulizade T.A. Problems of fraud qualification in the field of computer information // Russian Justice. 2019, no. 4, p. 21.
9. The official website of Rosstat [Electronic resource]. URL: https://rosstat.gov.ru (accessed 02/14/2025) .
10. Official website of the Federal Tax Service [Electronic resource] URL: https://www.nalog.gov.ru/rn77 (accessed 02/14/2025).
11. Regulations of the Bank of Russia dated April 8, 2020 No. 716-P "On Requirements for the Operational Risk Management System in a Credit Institution and a Banking Group", registered by the Ministry of Justice of the Russian Federation on June 3, 2020 No. 58577 (further on — Regulation of the Bank of Russia No. 716-P).
12. Semeko G.V. Information security in the financial sector: cybercrime and counteraction strategy // Social innovations and social sciences. Moscow: INION RAS, 2020, no. 1, pp. 77–79.
13. Kharitonov A.N. Qualification of fraud in the field of computer information / A.N. Kharitonov, E.V. Nikulchenkova // Russian Justice. 2019, no. 11, pp. 35–29.
14. INFOWATCH Investigation Center [Electronic resource]. URL: https://www.infowatch.ru (date accessed 02/28/2025).
15. The number of cyber attacks on the financial sector has increased by a quarter over the year – report of the Solar Group [Electronic resource] URL: https://rt-solar.ru/events/

13. *Харитонов А.Н*. Квалификация мошенничества в сфере компьютерной информации [Текст] / А.Н. Харитонов, Е.В. Никульченкова // Рос. юстиция. — 2019. — № 11. — С. 35–29.
14. Центр расследований INFOWATCH [Электронный ресурс]. — URL: https://www.infowatch.ru (дата обращения: 28.02.2025).
15. Число кибератак на финансовый сектор выросло за год на четверть — отчёт ГК «Солар» [Электронный ресурс]. — URL: https://rt-solar.ru/events/news/4076/?ysclid=m7xpashawl183417307 (дата обращения: 26.02.2025).

news/4076/?ysclid=m7xpashawl183417307 (accessed 02/26/2025).