УДК 343.34:004
ББК 67.408.135

ОРГАНИЗАЦИОННО-ПРАВОВЫЕ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ

Т. В. Филипенко
Институт экономических исследований (Донецк, Россия)

В современном цифровом мире, где информационные данные и компьютерные системы играют ключевую роль, кибербезопасность приобретает первостепенное значение. Она включает в себя комплекс мер, направленных на защиту от киберугроз, таких как взлом, кража данных и другие злонамеренные действия, и является критически важной для обеспечения стабильности и безопасности бизнеса, государства и каждого пользователя. Для обеспечения кибербезопасности требуется слаженная работа технических специалистов, юристов, управленцев, политиков.

На пути к надежной защите от киберугроз стоит целый ряд организационно-правовых проблем, среди которых несовершенство законодательной базы, пробелы в правовом регулировании, недостаточная координация государственных органов и частных компаний, занимающихся кибербезопасностью, дефицит специалистов, недостаточное финансирование, низкая культура кибербезопасности.

Решение перечисленных проблем требует комплексного подхода, направленного на совершенствование законодательства, организационных структур и технических средств, внедрение новых технологий, повышение квалификации специалистов и осведомленности населения о киберугрозах. Только совместными усилиями государства, бизнеса и общества можно создать надежную систему кибербезопасности, способную защитить от современных киберугроз.

Ключевые слова: кибербезопасность, информационная безопасность, киберугрозы, кибермошенничество, кибератаки, компьютерные преступления

ORGANIZATIONAL AND LEGAL PROBLEMS OF ENSURING CYBERSECURITY

T. V. Filipenko
Institute of Economic Research (Donetsk, Russia)

In today's digital world, where information data and computer systems play a key role, cybersecurity is of paramount importance. It includes a set of measures aimed at protecting against cyberthreats such as hacking, data theft and other malicious activities, and is critically important for ensuring the stability and security of businesses, the state and every user. Cybersecurity requires the coordinated work of technical specialists, lawyers, managers, and politicians.

There are a number of organizational and legal problems on the way to reliable protection against cyberthreats, including imperfection of the legislative framework, gaps in legal regulation, insufficient coordination of government agencies and private companies involved in cybersecurity, shortage of specialists, insufficient funding, low culture of cybersecurity.

Solving these problems requires an integrated approach aimed at improving legislation, organizational structures and technical means, introducing new technologies, improving the skills of specialists and public awareness of cyberthreats. Only through the joint efforts of the state, business and society can a reliable cybersecurity system be created that can protect against modern cyberthreats.

Keywords: cybersecurity, information security, cyberthreats, cyberfraud, cyberattacks, computer crimes

Doi: https://doi.org/10.14258/ralj(2025)4.16

Современные информационные технологии кардинально меняют экономику, политику, государственное управление и общество, открывая новые перспективы для граждан. В России большинство людей имеют круглосуточный доступ к осуществлению разнообразных финансовых операций через интернет и мобильные приложения. Однако вместе с распространением компьютерных технологий растет и опасность киберпреступности, которая подрывает экономическую стабильность страны.

Вопросы кибербезопасности и киберпреступности рассматриваются в работах многих российских ученых, среди которых: М. С. Решетникова, И. А. Пугачева, В. В. Попов, Д. И. Филиппов, Е. В. Кунц, В. Ф. Джафарли, М. В. Финкель, Р. В. Мещеряков, А. Р. Маргамов, А. Р. Набиева, Р. Ф. Гуляутдинов, Т. И. Чембарисов [1–7] и др. Однако актуальность существующих проблем требует дальнейшего изучения организационно-правовых аспектов кибербезопасности.

В соответствии с национальным стандартом ГОСТ Р 56205–2014 кибербезопасность включает в себя «действия, необходимые для предотвращения неавторизованного использования, отказа в обслуживании, преобразования, рассекречивания, потери прибыли или повреждения критических систем или информационных объектов» [8].

Термин «кибербезопасность» тесно связан с термином «информационная безопасность», они часто используются как взаимозаменяемые, однако они не идентичны. Информационная безопасность имеет более широкую сферу действия, охватывая защиту всех данных организации как в цифровом, так и в аналоговом формате. Кибербезопасность, напротив, фокусируется на защите цифровой информации от угроз в киберпространстве.

Цель кибербезопасности заключается в минимизации рисков, связанных с киберугрозами, что включает в себя защиту от физического вреда, ущерба репутации, утечки критически важной информации, финансовых потерь и несоблюдения нормативных требований. Эти риски актуальны для любых систем, используемых в производстве, от отдельных устройств до сложных интегрированных сетей. Безопасное взаимодействие между этими системами, будь то через внутренние каналы или внешние интерфейсы, требует строгой аутентификации, надежной функциональности, эффективного управления и безопасного обмена данными. Поэтому основополагающими принципами кибербезопасности являются идентификация, аутентификация, отслеживаемость, авторизация, доступность и приватность.

Реализация киберугроз чревата серьезными последствиями. Помимо потери и изменения данных, злоумышленники могут получить доступ к конфиденциальной информации. В то время как некоторые инциденты могут быть относительно безобидными, другие наносят значительный ущерб и даже ставят под угрозу национальную безопасность.

Киберугрозы проявляются в виде вирусных атак, мошеннических операций с кредитными картами, кражи денег с банковских счетов, утечки конфиденциальных данных и сбоев в работе автоматизированных вычислительных систем. Эксперты в области информационных технологий и права выражают обеспокоенность тем, что компьютеры все чаще используются для совершения таких серьезных преступлений, как терроризм, шпионаж, финансовое мошенничество, кражи, распространение детской порнографии и другие противозаконные действия.

Наибольшему риску кибератак подвержены телекоммуникационные, финансовые, розничные и промышленные компании. Малый и средний бизнес также становится привлекательной целью для киберпреступников из-за их активной деятельности и одновременно слабой кибербезопасности и недостаточной оценки рисков. Переход на удаленную работу усугубляет ситуацию, расширяя периметр безопасности компаний за счет домашних сетей и личных устройств сотрудников, что делает их более уязвимыми.

Согласно отчету компании Verizon за 2024 г., человеческий фактор является основной уязвимостью в кибербезопасности: 68% утечек данных происходит из-за человеческих ошибок или невнимательности, а не из-за злонамеренных действий. Это означает, что существует огромный потенциал для снижения рисков кибербезопасности за счет повышения осведомленности сотрудников и улучшения обучения в этой области [9].

Основными видами киберугроз, представляющих серьезную опасность для организаций, являются программы-вымогатели, целевые кибератаки, DDoS-атаки, фишинг, инсайдерские (внутренние) угрозы [10, с. 39].

Программы-вымогатели, шифруя данные и требуя выкуп, могут парализовать работу целых компаний.

Целевые атаки, или APT (Advanced Persistent Threat — развитая устойчивая угроза), — это сложные, хорошо спланированные операции, включающие проникновение в корпоративную сеть, похищение конфиденциальной информации и сокрытие следов взлома. В целевых атаках могут использоваться и другие методы киберпреступности — фишинг, вымогательство и т. д. Хотя такие атаки часто приписывают государственным структурам или крупным корпорациям из-за их сложности и стоимости, однако даже небольшие компании с перспективными разработками могут стать их целью.

DDoS-атаки — это попытки вывести из строя компьютерную систему, такую как веб-сервер, путем перегрузки ее ресурсами. Злоумышленники генерируют огромное количество одновременных запросов, которые система не может обработать. В результате система перестает отвечать на запросы пользователей, что приводит к отказу в обслуживании. Особенно уязвимы к таким атакам компании, ведущие бизнес онлайн, и телекоммуникационные компании.

Фишинг (fishing — рыбалка) — это мошенническая тактика, при которой злоумышленник пытается обманом выманить у жертвы конфиденциальную информацию. Обычно это делается путем рассылки обманчивых электронных писем, которые выглядят как официальные сообщения. Эти письма содержат либо вредоносные файлы, либо ссылки на поддельные сайты, предназначенные для кражи личных данных.

Инсайдерские угрозы — это риски безопасности, возникающие изнутри организации. Они могут быть вызваны действиями сотрудников, как намеренными (например, кража данных), так и непреднамеренными (например, ошибки или случайная утечка информации).

Мировой ущерб от кибератак в 2024 г. оценивается в 9,22 трлн долларов США, прогнозируется, что к 2028 г. эта цифра достигнет 13,82 трлн долларов США [11]. Отмечается, что методы злоумышленников становятся все более совершенными, используются технологии искусственного интеллекта для атак на пользователей и компании.

По данным Министерства внутренних дел в 2024 г. кибермошенники нанесли ущерб россиянам на сумму 200 млрд руб., что на 36% больше, чем в 2023 г. Основной причиной роста ущерба стало увеличение хищений кредитных средств, что подтверждает приоритет финансовой выгоды для киберпреступников. Жертвами этих преступлений стали 448,9 тыс. чел. [12].

Вместе с удобствами, которые цифровые технологии принесли клиентам, пришел и значительный рост мошеннических действий. Это создало благоприятную почву для нелегальных участников финансового рынка и расцвета финансовых онлайн-пирамид. В настоящее время российские банки особенно уязвимы перед телефонным мошенничеством и аферами с банковскими картами.

По данным Центробанка России, в 2024 г. объем средств, похищенных мошенниками у клиентов банков, резко возрос, достигнув 27,5 млрд руб. Это на 74,4% превышает показатель 2023 г. Больше всего пострадали физические лица, потерявшие 26,9 млрд руб., в то время как потери юридических лиц составили 667 млн руб. При этом наблюдается смена приоритетов у злоумышленников. Если раньше они в основном нацеливались на прямое хищение денежных средств, то теперь все чаще используют сложные многоступенчатые схемы, направленные на подрыв доверия к организациям. В 2025 г. регулятор ожидает увеличения числа репутационных атак, включающих утечки данных, манипуляции с корпоративными системами и распространение информации, вызывающей общественное недоверие [13].

В настоящее время ведется работа по ужесточению ответственности финансовых учреждений за случаи мошенничества, связанные с переводами денежных средств клиентов. С июля 2024 г. банки обязаны возвращать деньги гражданам, которые были незаконно списаны с их счетов. Возврат средств осуществляется в тех случаях, если перевод был отправлен на мошеннический счет, зарегистрированный в Центральном банке, а также если операция была выполнена без предварительного уведомления клиента. В таких ситуациях финансовые организации обязаны вернуть деньги в течение 30 дней с момента получения заявления от гражданина [14].

В 2024 г. российские банки вернули клиентам 2,7 млрд руб. похищенных мошенниками средств, что составляет 9,9% от общего объема. Также банкам удалось предотвратить хищения 13,5 трлн руб. Кроме того, с июля 2025 г. вводится обязательная двухдневная задержка платежей, если получатель средств фигурирует в базе данных Банка России как участник мошеннических схем.

Для повышения безопасности денежных переводов Генпрокуратура РФ инициировала внедрение автоматизированной системы, блокирующей переводы на счета, фигурирующие в мошеннических схемах. Министерство цифрового развития РФ, в свою очередь, работает над созданием единой платформы для противодействия кибермошенничеству, которая позволит объединить и усилить существующие механизмы выявления и предотвращения подозрительных транзакций.

В юридической литературе выделяются следующие виды негативных последствий компьютерных преступлений:

1. Нарушение работоспособности систем: а) дестабилизация рабочих процессов, нарушение графиков и планов; б) ограничение доступа к системе для пользователей; в) повреждение аппаратного и программного обеспечения системы.

2. Материальный ущерб: утрата денежных средств, товарно-материальных ценностей, оборудования, конфиденциальной информации.

3. Потеря исключительных прав на использование информации, в том числе коммерческой тайны.

4. Нарушение прав интеллектуальной собственности, незаконное использование объектов авторского и смежных прав, патентных прав, прав на изобретения и других охраняемых законом прав.

По информации Positive Technologie наиболее распространенными последствиями успешных кибератак на бизнес являются утечка конфиденциальной информации (67%) и нарушение основной деятельности (44%) [15].

Оценка полного спектра последствий преступлений, совершаемых с использованием информационных технологий, является крайне сложной задачей. Причина в том, что эти последствия напрямую зависят от типа и ценности информации, ставшей объектом преступного воздействия. Масштаб ущерба в каждом конкретном случае определяется значимостью общественных отношений, которые призваны оптимизировать компьютерные технологии.

Кибератаки оказывают влияние не только на финансовые показатели деятельности организаций и компаний. Они могут разрушить доверие клиентов, ухудшить репутацию компании, привести к заметному снижению стоимости акций [1, с. 4122].

Компьютерные преступления совершаются как сотрудниками организации, так и посторонними лицами. Однако подавляющее большинство (94%) таких преступлений совершается внутренними пользователями, причем основная их часть (70%) приходится на обычных пользователей компьютерных систем, а 24% — на обслуживающий персонал.

В сфере компьютерных технологий наблюдается тенденция к росту злоупотреблений и увеличению наносимого ими вреда. Это обусловлено несколькими факторами:

— повсеместное распространение информационных технологий создает больше возможностей для злоумышленников;
— увеличение числа квалифицированных специалистов в области информационных технологий сопровождается увеличением числа потенциальных злоумышленников с необходимыми знаниями и навыками;
— законодательная база, регулирующая информационные отношения и безопасность, не успевает за развитием технологий и оставляет лазейки для злоумышленников;
— многие системы не имеют адекватных технических средств защиты информации, что делает их уязвимыми для атак;
— низкий уровень раскрываемости преступлений в сфере информационных технологий снижает риск наказания и стимулирует злоумышленников.

По данным Генеральной прокуратуры РФ раскрываемость кибермошенничеств в 2024 г. составила лишь 23% [16]. Решение этой проблемы требует комплексного подхода, включающего активизацию взаимодействия между различными ведомствами, подготовку квалифицированных кадров и повышение осведомленности граждан о киберугрозах.

В отличие от обычных преступлений, киберпреступления характеризуются беспрецедентной скоростью и масштабом распространения, стирая границы времени, географии и даже личности преступника. Если для совершения традиционного преступления, например кражи, требуется физическое проникновение в охраняемое место, то для киберпреступления достаточно компьютера, базовых знаний о компьютерных системах и специализированного программного обеспечения. Это позволяет злоумышленникам совершать преступления, не покидая своего дома и не сталкиваясь с физическими препятствиями.

Важной особенностью компьютерных преступлений является анонимность цифровой информации, что существенно затрудняет расследование. В отличие от традиционных преступлений, где используются методы идентификации, такие как анализ почерка или отпечатков пальцев, в цифровой среде электронные следы часто не содержат явных идентификаторов, делая их анализ крайне сложным.

Характерной чертой компьютерных правонарушений является широкий спектр используемых инструментов. Вместо привычного физического оружия злоумышленники применяют разнообразное программное обеспечение для осуществления цифровых вторжений.

Преступления, связанные со взломом и нарушением работы компьютерных систем, представляют серьезную опасность. Несмотря на отличие от традиционных криминальных деяний, потенциальный ущерб от таких атак может быть сравним с последствиями крупных техногенных катастроф.

В настоящее время в развитии информационных технологий и кибербезопасности важное место занимает использование искусственного интеллекта [5, с. 39], 44% организаций по всему миру внедряют его для выявления и предотвращения киберугроз. Российские компании также активно работают над технологиями, которые позволят с помощью искусственного интеллекта обнаруживать сетевые нападения, заражения вредоносным программным обеспечением и другие киберугрозы.

Использование искусственного интеллекта стало ключевым фактором в развитии IT-рынка и кибербезопасности. По данным исследований, 44% организаций по всему миру применяют ИИ для проактивного выявления и блокировки киберугроз. Российские компании также инвестируют в разработку систем искусственного интеллекта, способных автоматически обнаруживать сетевые атаки, вредоносное программное обеспечение и другие виды киберугроз [5, с. 41]. Например, в Сбербанке России нейросеть интегрирована в программное обеспечение, защищающее от утечки данных. В социальной сети «ВКонтакте» искусственный интеллект помогает выявлять и блокировать оскорбительные комментарии, предупреждает пользователей о подозрительных контактах. Почтовый сервис Mail.ru и социальная сеть «Одноклассники» применяет искусственный интеллект для борьбы с фишингом, спамом и для восстановления утраченного доступа к аккаунтам.

По прогнозам Центра стратегических разработок технологии искусственного интеллекта будут ежегодно расти на 24%, при этом их развитие тесно взаимосвязано с кибербезопасностью [17].

С учетом перечисленных факторов злоупотребления в сфере компьютерных технологий превратились в острую проблему, требующую срочных и скоординированных усилий общества и государства. Для эффективного решения этой проблемы необходимо глубокое понимание компьютерной преступности как социального явления и разработка не только методов расследования, но и, что особенно важно, превентивных мер, направленных на предотвращение таких преступлений и формирование системной стратегии противодействия [3, с. 100].

Целью государственных инициатив является создание безопасной, надежной и доступной цифровой экосистемы, отвечающей интересам всех пользователей [2, с. 1517]. В то же время в России отсутствует комплексная, официально утвержденная концепция кибербезопасности. Разработанный в 2010 г. соответствующий проект так и не был реализован. Регулирование в сфере кибербезопасности осуществляется посредством отдельных нормативных правовых актов, охватывающих различные аспекты информационной безопасности и деятельности в киберпространстве [18].

К таким документам можно отнести Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации, утвержденные Указом Президента РФ от 3 февраля 2012 г. № 803. Документ определяет критически важный объект инфраструктуры Российской Федерации как объект, отказ или прекращение работы

которого влечет за собой серьезные и долговременные последствия. К ним относятся: утрата управляемости, разрушение инфраструктурных элементов, нанесение непоправимого ущерба экономике (на национальном, региональном или местном уровне), а также значительное ухудшение условий безопасности жизнедеятельности населения. Установлено, что государственная политика направлена на минимизацию рисков, связанных с несанкционированным влиянием на системы управления производственными и технологическими процессами этих объектов, и на смягчение потенциальных негативных последствий такого воздействия.

Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» определяет, какие информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления считаются объектами критической информационной инфраструктуры. К ним относятся системы, работающие в таких жизненно важных сферах, как здравоохранение, наука, транспорт, связь, энергетика, финансовый сектор, топливно-энергетический комплекс, атомная промышленность, оборона, космическая отрасль, горнодобывающая, металлургическая и химическая промышленность. Закон устанавливает основные принципы обеспечения безопасности критической информационной инфраструктуры, определяет полномочия государственных органов в этой области, а также права, обязанности и ответственность организаций, эксплуатирующих эти системы. Для защиты критической информационной инфраструктуры закон предусматривает ряд мер, включая категоризацию объектов по степени значимости, ведение реестра значимых объектов критической информационной инфраструктуры, оценку уровня их защищенности, осуществление государственного контроля и создание специализированных систем безопасности.

Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (Концепция ГосСопка), утвержденная Указом Президента РФ от 12 декабря 2014 г. № К 1274, определяет цели, задачи, принципы построения и функционирования соответствующей государственной системы, а также необходимые виды обеспечения для ее создания и эксплуатации. ГосСопка представляет собой иерархически организованную сеть государственных и коммерческих центров, осуществляющих непрерывный обмен информацией об инцидентах информационной безопасности и методах их нейтрализации.

Доктрина информационной безопасности Российской Федерации, утвержденная Указом Президента РФ от 5 декабря 2016 г. № 646, определяет состав и структуру информационной сферы, включая информацию, объекты информатизации, информационные системы, веб-ресурсы, средства связи, информационные технологии и субъекты, осуществляющие деятельность в данной сфере. Доктрина устанавливает, что обеспечение информационной безопасности является комплексной задачей, требующей реализации взаимосвязанных мер правового, организационного, оперативно-разыскного, разведывательного, контрразведывательного, научно-технического, информационно-аналитического, кадрового и экономического характера. Целью этих мер является прогнозирование, выявление, сдерживание, предотвращение и отражение информационных угроз, а также устранение последствий их реализации и регулирование общественных отношений в информационной сфере.

Согласно Стратегии национальной безопасности Российской Федерации, утвержденной Указом Президента РФ от 2 июля 2021 г. № 400, ключевой целью в сфере информационной безопасности является укрепление суверенитета РФ в информационном пространстве. Для ее достижения, помимо противодействия киберпреступности и защиты критической инфраструктуры, особое внимание уделяется развитию и внедрению передовых технологий в сфере информационной безопасности. В частности, планируется активное использование искусственного интеллекта и квантовых вычислений для создания более эффективных средств и методов защиты.

Указ Президента Российской Федерации от 30 марта 2022 г. № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации» ввел прямой запрет на приобретение и использование иностранного программного обеспечения и программно-аппаратных комплексов на соответствующих объектах, за исключением согласованных случаев. Ключевая задача заключается в переходе на преимущественное использование отечественных разработок.

В соответствии с Концепцией формирования и развития культуры информационной безопасности граждан Российской Федерации, утвержденной Распоряжением Правительства РФ от 22 декабря 2022 г. № 4088-р, поставлена задача повышения уровня информационной безопасности граждан РФ. Ключевой целью является формирование у населения компетенций, необходимых для противодействия современным угрозам, включая информационно-психологические. Реализация концепции предполагает проведение регулярных информационных кампаний, ориентированных на распространение знаний о правилах личной информационной безопасности в доступной и ненавязчивой форме, с использованием популярных интернет-ресурсов.

Для снижения уровня киберпреступности и дальнейшего укрепления кибербезопасности в стране представляется необходимым:

— продолжить разработку законодательства, охватывающего все аспекты кибербезопасности;
— создать единый координационный центр, обеспечивающий согласованную работу государственных структур и частного сектора в сфере кибербезопасности;
— увеличить количество образовательных программ по кибербезопасности и повысить привлекательность работы в этой сфере;
— обеспечить достаточное финансирование для поддержания и развития системы кибербезопасности;
— проводить образовательные мероприятия для сотрудников организаций и населения для повышения их цифровой грамотности и безопасного поведения в сети;
— укреплять международное сотрудничество для борьбы с киберпреступностью и разработки единых международных стандартов кибербезопасности.

Таким образом, *б*орьба с киберпреступностью и обеспечение кибербезопасности требует комплексного подхода, включающего усиление государственной защиты, повышение цифровой грамотности населения и создание современной системы кибербезопасности, основанной на соответствующем законодательстве и передовых информационных технологиях.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Решетникова М. С., Пугачева И. А., Попов В. В. Киберугрозы: фактор неопределенности цифровой экономики // Креативная экономика. 2022. Т. 16, № 11. С. 4113–4130.

2. Филиппов Д. И. Финансовые инновации в условиях развития цифровой экономики // Креативная экономика. 2019. Т. 13, № 8. С. 1503–1520.

3. Кунц Е. В. Противодействие современным киберпреступлениям // Российско-Азиатский правовой журнал. 2025. № 1. С. 97–104.

4. Джафарли В. Ф., Финкель М. В. Актуальность обеспечения криминологической кибербезопасности в предпринимательской деятельности // Ученые труды Российского университета адвокатуры и нотариата им. Г. Б. Мирзоева. 2024. № 2. С. 79–82.

5. Мещеряков Р. В. Вопросы безопасности систем искусственного интеллекта // Искусственный интеллект: теория и практика. 2023. № 4. С. 38–41.

6. Маргамов А. Р., Набиева А. Р. Развитие взаимодействий органов власти с получателями государственных услуг с учетом рисков кибербезопасности // Конкурентоспособность в глобальном мире: экономика, наука, технологии. 2024. № 5. С. 49–51.

7. Гуляутдинов Р. Ф., Чембарисов Т. И. Тенденции развития кибермошенничества в России // Евразийский юридический журнал. 2023. № 2. С. 256–258.

8. Национальный стандарт Российской Федерации «Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 1–1. Терминология, концептуальные положения и модели»: ГОСТ Р 56205–2014 (IEC/TS 62443–1–1:2009) от 01.01.2016 // Электронный фонд правовых и нормативно-технических документов. URL: https://docs.cntd.ru/document/1200114169 (дата обращения: 30.05.2025).

9. Отчет о расследовании утечки данных за 2024 год: Большинство нарушений связаны с незлонамеренным человеческим фактором. URL: https://newsletter.radensa.ru/archives/6363 (дата обращения: 30.05.2025).

10. Филипенко Т. В. Киберугрозы экономической безопасности государства // Устойчивое развитие науки и образования. 2023. № 12. С. 38–42.

11. Ущерб от киберпреступлений вырастет на треть за следующие 4 года // ИММР. URL: https://worldmarketstudies.ru/article/userb-ot-kiberprestuplenij-vyrastet-na-tret-za-sleduusie-4-goda/ (дата обращения: 30.05.2025).

12. Ущерб от действий кибермошенников в РФ в 2024 г. вырос на 36%, до 200 млрд руб. // Интерфакс. URL: https://www.interfax.ru/russia/1009710 (дата обращения: 30.05.2025),

13. ЦБ зафиксировал рекордную сумму хищений у банковских клиентов в 2024 году // РБК. URL: https://www.rbc.ru/finances/18/02/2025/67b489749a794780d1527516? ysclid=mb7nj8b38f464513655 (дата обращения: 30.05.2025).

14. О внесении изменений в Федеральный закон «О национальной платежной системе» : Федеральный закон от 24.07.2023 № 369-ФЗ // Гарант. URL: https://base.garant.ru/407426196/ (дата обращения: 30.05.2025).

15. Positive Technologies: четыре из пяти атак носят целенаправленный характер. URL: https://telecomdaily.ru/news/2023/08/29/positive-technologies-chetyre-iz-pyati-atak-nosyat-celenapravlennyy-harakter (дата обращения: 30.05.2025).

16. Генпрокуратура России оценила раскрываемость кибермошенничеств в 23% // Интерфакс. URL: https://www.interfax.ru/russia/1009713 (дата обращения: 30.05.2025).

17. Что будет с кибербезопасностью в 2024 году // РБК. URL: https://trends.rbc.ru/trends/innovation/657718709a7947ed6188d010 (дата обращения: 30.05.2025).

18. Стратегии кибербезопасности: Аналитический отчет InfoWatch. URL: https://www.infowatch.ru/sites/default/files/publication_file/analiticheskiy-otchet-strategii-kiberbezopasnosti.pdf ?ysclid=m1wgqyl832715941524 (дата обращения: 30.05.2025).