УДК 330.341.4

БЕЗОПАСНОСТЬ ЦИФРОВОЙ ЭКОНОМИКИ РОССИИ И ЕЕ РЕГИОНОВ

Н.В. Яковлева
Иркутский государственный университет путей сообщения, Иркутск, email: yako.n.fbu@yandex.ru

Аннотация. *Цифровая трансформация как неотъемлемая часть современного витка НТР является необходимым фактором экономического роста. В статье выделены и исследованы группы угроз безопасности цифровой экономики, с которыми сталкивается Россия и отдельные ее регионы. Особое внимание уделено угрозе экономических и политических войн, которые рождают киберугрозы для РФ. Исследованы проявления киберугроз для нашей страны в целом, а также специфика их проявления на региональном уровне, в частности в Иркутской области. Исследуется динамика основных статистических показателей степени подверженности населения и отраслей экономики различным видам кибератак с 2018 по 2022-2024 гг., а также дифференциация проявления киберугроз в различных субъектах РФ. По результатам исследования выявлены системные причины высокого уровня проявления киберугроз в Иркутской области. Рассматриваются меры регионального Правительства по противодействию киберугрозам. В заключение дается оценка трансформации и развития киберугроз для РФ и предлагаются возможные направления решения проблем для повышения безопасности цифровой экономики Иркутской области.*

Ключевые слова*: цифровая экономика, цифровая трансформация, киберугрозы, экономическая безопасность, региональные программы.*

SECURITY OF THE DIGITAL ECONOMY OF RUSSIA AND ITS REGIONS

N.V. Yakovleva
Irkutsk State University of Railway Engineering, Irkutsk, email: yako.n.fbu@yandex.ru

Abstract. *Digital transformation as an integral part of the modern round of scientific and technological revolution is a necessary factor for economic growth. The article identifies and examines groups of threats to the security of the digital economy that Russia and its individual regions face. Particular attention is paid to the threat of economic and political wars that give rise to cyber threats for the Russian Federation. Manifestations of cyber threats for our country as a whole, as well as the specifics of their manifestation at the regional level, in particular in the Irkutsk region, are studied. The dynamics of the main statistical indicators of the degree of exposure of the population and sectors of the economy to various types of cyber attacks from 2018 to 2022-2024, as well as the differentiation of the manifestation of cyber threats in various constituent entities of the Russian Federation are studied. Based on the results of the study, systemic reasons for the high level of manifestation of cyber threats in the Irkutsk region were identified. Measures of the regional Government to counter cyber threats are considered. In conclusion, an assessment of the transformation and development of cyber threats for the Russian Federation is given and possible directions for solving problems to improve the security of the digital economy of the Irkutsk region are proposed.*

Keywords: *digital economy, digital transformation, cyber threats, economic security, regional programs.*

Дата поступления статьи в редакцию: 07.07.2025
Дата принятия статьи в печать: 07.08.2025

Введение

Цифровые технологии значительно изменили процессы и инфраструктуру экономических систем государств. Цифровая трансформация определена в качестве приоритетной цели экономического роста страны в соответствии с Указом Президента РФ от 2020 года «О национальных целях развития РФ». Системный подход государства к цифровой трансформации экономики основан на официальных стратегических документах, в которых закреплено понимание цифровой экономики как деятельности, где данные в цифровой форме являются основным ресурсом. Так, в «Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» подчеркивается, что цифровая экономика формируется на основе обработки больших объемов данных и применения результатов их анализа для повышения эффективности хозяйствования. В условиях роста киберпреступлений в геометрической прогрессии актуальность защиты данных приобретает особое значение.

Цель исследования

Исследование цифровой экономики в России и ее регионах на современном этапе и выявление динамических тенденций угроз и системных причин, лежащих в основе их возникновения.

Объекты и методы исследования

В качестве объекта исследования выбрана цифровая экономика России как система. Предметом исследования выступают угрозы безопасности в цифровой экономике России и ее регионов. На основе анализа и синтеза всесторонних аспектов развития цифровизации экономической системы страны мы исследовали причины и факторы, влияющие на возникновение и динамику объемов и количества угроз безопасности в цифровой экономике, в частности для домохозяйств.

Результаты и их обсуждение

Безопасность цифровой экономики обеспечивается рядом государственных структур, отвечающих за различные сферы цифровизации социально-экономической системы России: Министерство цифрового развития РФ, Банк России, Федеральная служба по техническому и экспортному контролю РФ, Федеральная служба безопасности РФ. Тем не менее, стремительный рост киберпреступности свидетельствует о нерешенности ряда вопросов национальной безопасности в цифровой сфере. Базовые основы обеспечения безопасности в области ИТ заложены в «Доктрине информационной безопасности Российской Федерации». Также в рамках национальной программы «Цифровая экономика Российской Федерации» выделен федеральный проект «Информационная безопасность», целью которого является обеспечение устойчивости и безопасности информационной инфраструктуры, конкурентоспособности отечественных разработок и технологий информационной безопасности и построение эффективной системы защиты прав и законных интересов личности, бизнеса и государства от угроз информационной безопасности. Вопросы безопасности информации в процессе цифровой трансформации регламентируют Федеральные законы: «О персональных данных», «Об информации, информационных технологиях и о защите информации», «О безопасности критической информационной инфраструктуры Российской Федерации» и др.

Открывая новые возможности для роста и модернизации, цифровизация экономики способствует возникновению ряда серьезных опасностей экономическим интересам как национальной безопасности, так и безопасности частных юридических и физических лиц. Опасность, у которой имеется точно установленный источник возникновения, может пониматься как угроза. Обобщенно виды угроз в цифровой экономике государства можно представить в виде пяти групп.

Первая группа – угрозы цифрового неравенства способствуют дестабилизации структуры экономики страны. Доступ к цифровым технологиям различается в зависимости от региона, уровня доходов и образования населения. Крупные агломерации имеют развитую цифровую инфраструктуру, тогда как сельские и удалённые районы часто остаются в стороне от прогресса, что усиливает социально-экономический разрыв [1].

Автоматизация производства и внедрение искусственного интеллекта постепенно вытесняют традиционные профессии, особенно в сферах низкоквалифицированного труда. Это приводит к увеличению уровня безработицы среди определённых групп населения и требует перестройки системы профессионального образования: развития новых компетенций, поддержки программ переквалификации, создания новых рабочих мест в области цифровой экономики [2]. Кроме того, повышается риск монополизации цифрового рынка. Крупные технологические компании могут получить чрезмерное влияние, диктуя условия рынку, ограничивая конкуренцию и влияя на политику государств.

Вторая группа угроз – политические и правовые угрозы, которые могут затронуть фундаментальные принципы государственного управления. Например, через цифровые платформы может осуществляться влияние на электоральные процессы, манипуляция общественным мнением, распространение дезинформации.

Российская правовая система часто не успевает за развитием цифровых технологий. В результате возникает правовой вакуум в таких сферах, как защита персональных данных, регулирование цифровых валют, искусственного интеллекта и платформенных компаний. Отсутствие эффективных правовых механизмов повышает риск нарушений прав граждан и усугубляет проблемы безопасности.

Кроме того, развитие цифровых платформ приводит к появлению новых угроз национальной безопасности: иностранные цифровые сервисы могут собирать данные о гражданах, контролировать информационные потоки и влиять на стратегические решения [3].

Третья группа угроз – угрозы экономических и информационных войн. В современных условиях информационное пространство становится новым полем военных действий. Кибератаки способны нарушить функционирование государственных систем управления, объектов критической инфраструктуры, финансовых институтов.

Распространение дезинформации, кибершпионаж, цифровые диверсии становятся инструментами политической и экономической борьбы. Информационные войны могут подрывать стабильность внутри страны, ослаблять доверие граждан к властям, провоцировать социальные конфликты. Учитывая зависимость от цифровых технологий, необходимо усиление мер по кибербезопасности, развитие национального суверенитета в информационной сфере и формирование системы быстрого реагирования на киберугрозы.

Четвертая группа – социокультурные угрозы. Цифровизация затрагивает не только экономику и политику, но и основы общественной жизни. Массовый переход на удалённую работу, дистанционное обучение, онлайн-коммуникации изменяет характер межличностных отношений.

Проблемы социальной изоляции становятся всё более актуальными: утрата живого общения ведет к росту психологических расстройств, чувству одиночества, снижению качества социальных связей. Молодёжь, выросшая в цифровой среде, формирует новые модели поведения, зачастую отрываясь от традиционных культурных норм [4].

Кроме того, цифровые технологии влияют на культурное наследие: традиционные формы искусства, коммуникации и образования подвергаются трансформации или маргинализации. Это требует осмысленного подхода к сохранению культурной идентичности в условиях цифрового общества.

Пятая группа – технологические угрозы, представляющие для России особую опасность, так как они выражаются в технологической зависимости от других государств. Использование зарубежного программного обеспечения, оборудования и сервисов делает экономику уязвимой перед внешними санкциями, отключением от технологических платформ и сетей.

Недостаточное развитие отечественных технологий в таких областях, как микроэлектроника, искусственный интеллект и кибербезопасность, ограничивает возможности обеспечения суверенитета в цифровой сфере. Также существует риск системных сбоев: быстрое внедрение новых технологий в том числе в процессе импортозамещения без должной адаптации бизнес-процессов и инфраструктуры может привести к технологическим катастрофам, утрате данных, параличу важных отраслей экономики [5,6].

Цифровая трансформация экономики является мощным драйвером роста для России, но сопровождается комплексом серьёзных киберугроз. В 2024 году зарегистрировано более 640 тыс. киберпреступлений, с общим ущербом свыше 170 млрд. руб. Как мы отмечали выше, киберугрозы исходят от злоумышленников в результате реализации второй, третьей, пятой группы, рассмотренной нами ранее классификации угроз [7].

Рассматривая понятие киберугроз, нужно отметить характерные черты: они могут быть направлены на нарушение работы систем и/или кражу информации и/или повреждение информационных ресурсов. Также киберугрозы реализуются на практике в различных формах в виде конкретных действий, т.е. кибератак, в т.ч. включая распространение вредоносного программного обеспечения, фишинговые атаки, DDoS-атаки и несанкционированный доступ к сетям или базам данных. Часто кибератаки направлены на получение финансовой выгоды, или же, с чем столкнулась сейчас Россия, – на подрыв репутации организаций или государств, кражу интеллектуальной собственности или вмешательство в критическую инфраструктуру [5, 6, 8].

Одним из эффективных способов оценки уровня киберугроз является использование количественных показателей, отражающих масштаб и динамику инцидентов в сфере информационной безопасности. Это позволяет не только выявить наиболее уязвимые направления, но и определить возможный размер ущерба, приоритетные меры для повышения устойчивости цифровой экономики и объем расходов на них.

В 2024 году общее число кибератак на российский бизнес выросло до 130 000 случаев, т.е. в 2,5 раза чем годом ранее. Среднемесячное количество атак составило 10 000 случаев, максимальное количество отмечалось в феврале (12 тыс.), мае (19 тыс.) и июне (13 тыс.). Количество высококритичных инцидентов достигло 26 000, каждый пятый из которых потенциально мог нанести ущерб более 1 млн руб. Совокупный предотвращённый ущерб составил 26 млрд руб. [9]

Если рассматривать кибератаки в отраслевом разрезе экономики, то самой атакуемой стала промышленность. На нее приходилось более 31% от общего числа всех атак и 28% от общего числа высококритичных атак. Почти половина (45%) всех атак на данную отрасли приходилась на выходные и праздничные дни. При этом доля критических инцидентов в ночное время заметно возрастала: с 12% в рабочие часы компаний до 25% – в ночные. Основная цель кибератак в промышленной отрасли – это промышленный

шпионаж, поскольку вредоносное ПО, используемое в ходе этих кибератак, в 38% случаев имела функциональность кражи учетных данных и шпионажа, и только в 19% случаев – шифрования данных [10].

Также активным кибератакам подвергалась в 2024 сфера ИТ. На нее пришлось 20% от общего числа атак и 14% от общего числа высококритичных инцидентов. Были зафиксированы крупные взломы производителей отечественного ПО. Аналитики связывают это с растущей популярностью попыток атак на российские компании через их ИТ-подрядчиков – вендоров, системных интеграторов и т.п. В 2024 году количество таких инцидентов выросло примерно на 50%.

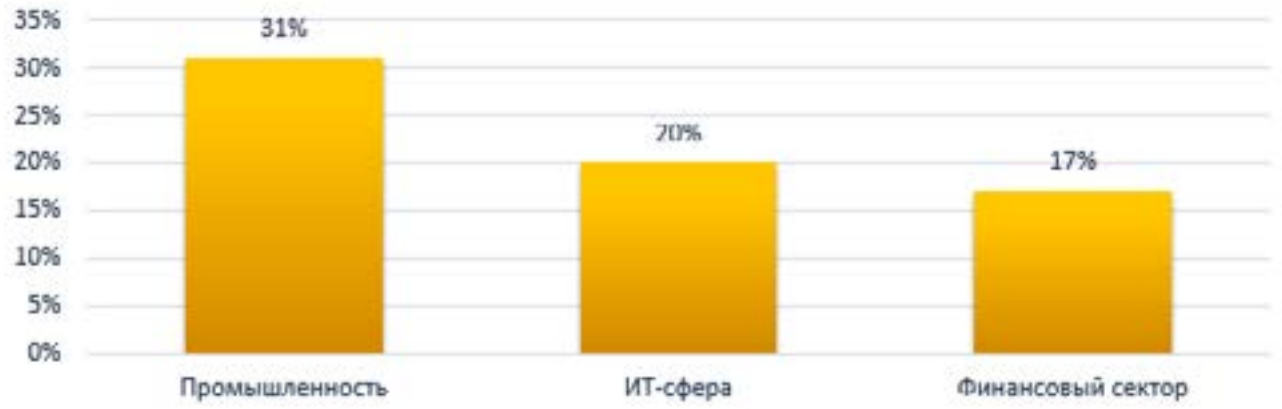

Рис. 1. *Распределение кибератак по секторам в России за 2024 г. [10]*

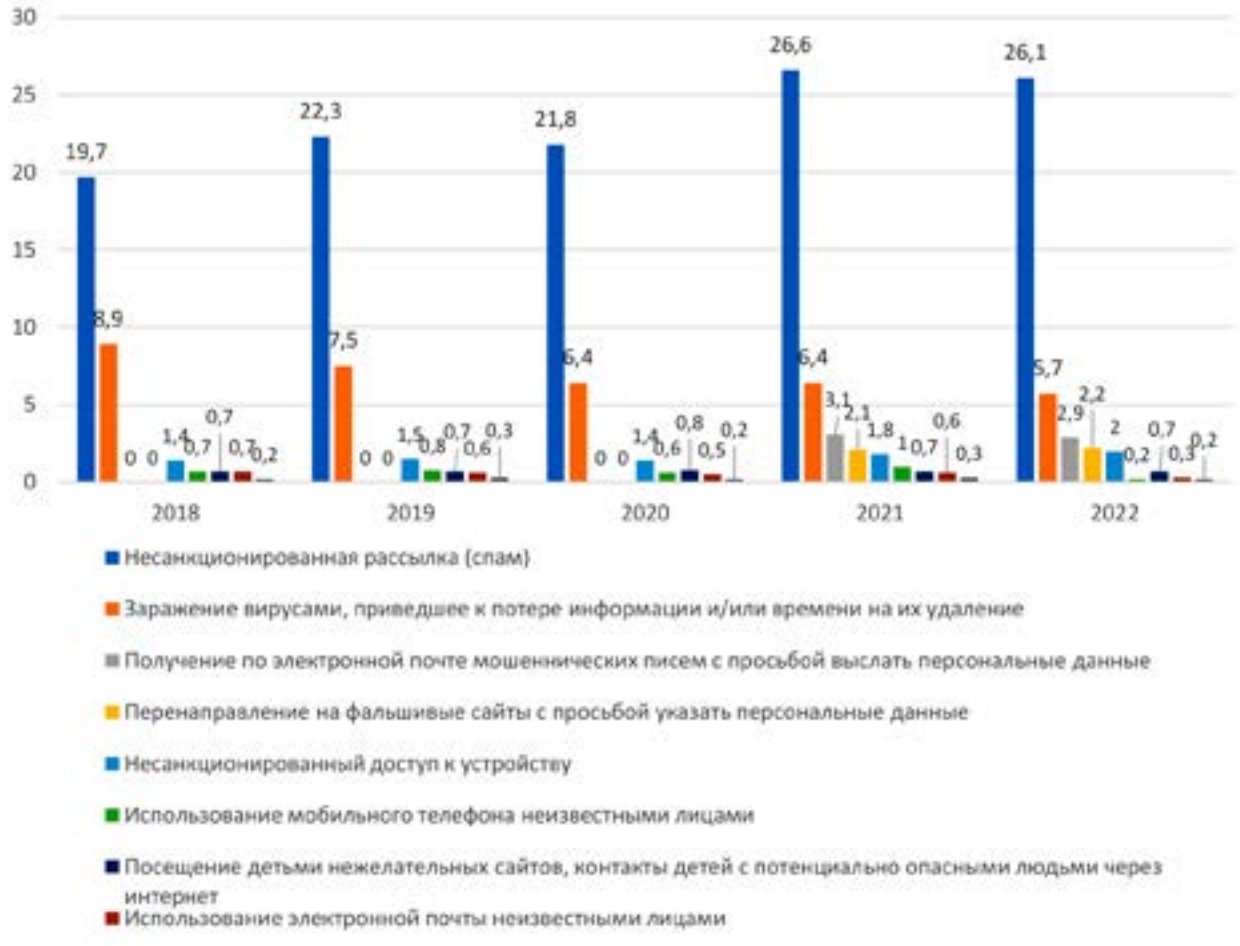

Рис. 2. *Динамика показателей, оценивающих столкновение населения с угрозами информационной безопасности при использовании интернета в России [12]*

На третьем месте по количеству предотвращенных инцидентов оказался финансовый сектор, В 2024 году он испытал на себе 17% от общего числа атак, в том числе высокой критичности [10]. В качестве ключевого тренда киберугроз в данной сфере аналитики указывают применение атакующих технологий искусственного интеллекта. Они помогают хакерам быстро кастомизировать атаку вплоть до фишинговых писем, созданных под конкретного сотрудника, а также проводить ряд непрерывных попыток взлома банков разнообразными методами в течение длительного времени (рис. 1).

Угрозы экономических и информационных войн на сфере цифровой экономики, как правило, связаны с мошенничеством и финансовыми рисками. Рассмотрим проявления таких угроз в виде кражи персональных и платежных данных, неправомерного доступа к банковским счетам, проведения несанкционированных транзакций, а также масштабных схем интернет-мошенничества. Особенно остро данная проблема стоит в условиях активного распространения онлайн-сервисов, включая электронную коммерцию, онлайн-банкинг и государственные цифровые услуги [11]. Актуальность данных угроз подтверждается статистикой. На рисунке 2 представлены показатели, отражающие, с какими формами информационных угроз сталкивалось население России при использовании интернета за период с 2018 по 2022 год.

Анализ динамики показателей, оценивающих столкновение населения с угрозами информационной безопасности при использовании интернета в России (в процентах от численности населения в возрасте 15–74 лет), показывает несколько ключевых тенденций за период с 2018 по 2022 годы.

Несанкционированная рассылка (спам): показатель демонстрирует устойчивый рост, начиная с 19,7% в 2018 году и достигая 26,6% в 2021 году, с небольшим снижением до 26,1% в 2022 году. Это свидетельствует о постоянной проблеме спама, которая продолжает оставаться актуальной для пользователей.

Заражение вирусами: показатель по этому типу угроз имеет тенденцию к снижению – с 8,9% в 2018 году до 5,7% в 2022 году. Это может указывать на улучшение знаний пользователей о кибербезопасности и более эффективные меры защиты.

Несанкционированный доступ к устройству: показатель постепенно увеличивается с 1,4% в 2018 году до 2,0% в 2022 году, что может говорить о росте случаев кибератак.

Мошеннические письма и фальшивые сайты: эти угрозы начали фиксироваться в 2021 году, с показателями 3,1% и 2,1% соответственно. В 2022 году наблюдается небольшое снижение (до 2,9% и 2,2%), что может говорить о том, что мошеннические схемы становятся более распространенными, но пользователи начинают лучше их распознавать.

Использование мобильного телефона неизвестными лицами: здесь наблюдается значительное снижение в 2022 году до 0,2%, после пика в 1,0% в 2021 году. Это может свидетельствовать о снижении случаев использования мобильных устройств для мошеннических действий.

Посещение детьми нежелательных сайтов и контакты с опасными людьми: этот показатель остается стабильным на уровне около 0,7%, что указывает на необходимость продолжения работы по защите детей в интернете.

Хищение денежных средств и персональных данных: показатель остается низким и стабильным (0,2%-0,3%), что может говорить о том, что такие случаи не так распространены среди опрошенных.

Общий показатель угроз возрос с 27,9% в 2018 году до 34,3% в 2021 году, но затем снизился до 32% в 2022 году. Это может указывать на то, что несмотря на рост осведомленности о киберугрозах и совершенствование защиты, данные проблемы останутся актуальными на перспективу.

В целом, представленная динамика показывает рост определенных типов угроз, преступные элементы совершенствуют свои методы и инструменты синхронно с развитием цифровой трансформации, а также использование социальной инженерии по-прежнему сохраняет популярность (98% киберпреступлений в отношении населения совершено данным способом).

Важность работы на федеральном уровне по повышению осведомленности пользователей о кибербезопасности и внедрения опережающих мер защиты не вызывает сомнения. Но учитывая дифференциацию социально-экономического развития территорий России, специфика объемов и силы давления цифровых угроз в регионах имеет свою специфику. Рассмотрим несколько рандомно выбранных регионов и сравним с общероссийскими значениями по показателю доли населения, столкнувшегося с угрозами информационной безопасности (рис. 3). Доля населения, столкнувшаяся с угрозами информационной безопасности, в целом по России в 2024г. составляет 47,9%, в Республике Крым 28,2%, в Новосибирской области 29,9%, в Иркутской области 47,8%.

С точки зрения вида угроз, лидирует получение спама, достигая 41,6% на уровне РФ в целом. В Новосибирской области и республике Крым примерно одинаковые значения – 27% и 24% соответственно, в Иркутской области этот показатель практически в 1,5 раза выше – 41,2%. Наименьшая доля

населения сталкивалась с кражей денежных средств с банковских карт в исследуемых регионах, и она составляет примерно одинаковую долю в 0,2%. В Республике Крым большая доля населения подвергалась перенаправлению на поддельные сайты с просьбой указать личную информацию, заражению вирусами и получению мошеннических писем и сообщений, чем Новосибирской области. Но в последней наблюдается превышение доли населения подвергшихся взлому учетных записей, над данным показателем Республики Крым. Иркутская область имеет наихудшие значения среди представленных регионов по всем видам угроз. Нужно отметить, что только в Иркутской области доля населения, подвергшегося получению мошеннических писем и сообщений, значительно (на 6%) превышает общероссийский уровень. А по получению спама практически равна общероссийскому уровню. Рассмотрим динамику по данным угрозам в Иркутской области за ряд последних лет (рис. 4). Доля населения, столкнувшегося с угрозами информационной безопасности, в Иркутской области возросла более чем на 10% и достигла 47,9% в 2024 г., по сравнению с предыдущими годами (34,4% в 2023 г.) При этом доля населения, использующая средства защиты от информационных угроз, выросла всего на 1,1%, достигнув 69,1%.

Рис. 3. *Доля населения, столкнувшегося с угрозами информационной безопасности в ряде регионов и в РФ в 2024 гг. (в %, в возрасте 15 лет и старше) [12-14]*

Для выявления причин такого роста, выделим ряд тенденций: в 2024 г. резко выросла доля населения, столкнувшаяся с получением спама и мошеннических писем и сообщений, но затормозился рост заражения устройств вирусами. Доля населения, столкнувшаяся с перенаправлением на поддельные сайты с просьбой указать личную информацию начала незначительно снижаться (на 0,3%). Практически в половину снизилась доля населения, столкнувшаяся со взломом учетных записей, и в 4 раза снизилась доля населения, столкнувшаяся с кражей денежных средств с банковских карт. Последнюю тенденцию можно связать с введенными банками правилами предоставления кредитов с периодом «охлаждения» и тщательно проводимой работой по предупреждению таких хищений путем прямого взаимодействия с клиентом и инструктажа о возможных рисках и угрозах. Также этому способствовало расширение использования технологических инноваций в области искусственного интеллекта в онлайн-банкинге, которое позволяет отслеживать и блокировать мошеннические сообщения и звонки [15]. Тем не менее, если оценивать эту угрозу по объему, отметим, что в 2024 году объем ущерба составил 27,5 млрд руб., что на 74,4% больше, чем в 2023 году (15,8 млрд. руб.). При этом у физических лиц было похищено 26,9 млрд руб., что составляет практически 98% от общего объема ущерба [16].

Рис. 4. *Динамика доли населения, столкнувшегося с угрозами информационной безопасности в Иркутской области в период 2022-2024 гг. (в%, в возрасте 15 лет и старше) [13]*

Рост доли населения подвергающегося информационной безопасности в Иркутской области связан также с активным развитием цифровой инфраструктуры. По данным Банка России к 2024 г. в регионе выросли подключения к интернету в 3 раза, количество точек с сервисом «наличные на кассе» в 1,8 раза [17]. Низкая финансовая доступность территорий области (53%) из-за сокращения сети банков и недостатка кадров в банковской сфере тормозит повышение финансовой грамотности населения. Нежелание бизнеса работать легально, не достаточное или не качественное покрытие интернетом территории области, удерживает высокую долю наличных расчетов в регионе. Тем не менее, работа правительства Иркутской области в этом направлении ведется в рамках федеральной программы «Устранение цифрового неравенства 2.0» национального проекта «Цифровая экономика Российской Федерации»: совместно с сотовыми операторами прорабатываются дополнительные возможности обеспечения связью отдаленных и малочисленных населенных пунктов региона, например, предусмотрены субсидии из областного бюджета на софинансирование расходных обязательств муниципальных образований. К 2024 г. доля домохозяйств с доступом в Интернет возросла с 2018 г. на 19,8% и достигла 94,3% от общей численности домохозяйств [17].

В рамках национальной программы «Цифровая экономика Российской Федерации» в исследуемом субъекте РФ реализовывались пять региональных проектов «Информационная безопасность», «Информационная инфраструктура» «Цифровые технологии», «Цифровое государственное управление», «Кадры для цифровой экономики». Правительство Иркутской области на основе составленного оперативного рейтинга показателей эффективности и результативности руководителей цифровой трансформации выявило, что цели в области безопасности были достигнуты всего лишь на 70% [17]. Основные причины такой ситуации видятся в недостатке соответствующих кадров и необходимых объемов финансирования в условиях активных инфляционных процессов.

С 2024 г. в Иркутской области реализуется государственная программа «Цифровое развитие, связь и телекоммуникации», целями которой являются:

– уровень «цифровой зрелости» ключевых отраслей экономики, социальной сферы, и государственного управления достигнет 100% к 2030 году;

– уровень удовлетворенности граждан предоставления государственных и муниципальных услуг не менее 90% ежегодно к 2030 году;

– увеличение доли домохозяйств, имеющих доступ в Интернет, до 97% к 2030 году; и др. [18].

Финансирование программы осуществляется практически полностью за счет областного бюджета в размере 1,8 млрд. руб. ежегодно, до 2026 г. Технологические инновации, предусмотренные програм-

мой, в виде использования спутниковых навигационных технологий обеспечит мониторинг и контроль за критически важными, потенциально опасными и социально значимыми объектами на территории Иркутской области, а также принесет ощутимы экономический эффект в результате повышения качества расходования бюджетных средств и увеличения поступлений в областной бюджет.

Выводы

В заключение необходимо отметить, что рост давления угроз на цифровую инфраструктуру растет: традиционные атаки с целью хищения средств постепенно уходят в прошлое, на их место приходят многоэтапные схемы с целью подрыва доверия к организациям через манипуляцию данными и информационное давление, сопровождающиеся утечкой данных, манипуляцией с корпоративными системами и публикацией данных, вызывающих общественное недоверие. В данном случае совместные усилия федеральных регуляторных институтов – государственных структур (отмеченных в начале нашей статьи) с региональным Правительством позволят синхронизировать мероприятия по цифровой финансовой доступности с целевыми программами в области цифровой безопасности и адаптировать меры к потребностям населения и бизнеса конкретных населенных пунктов, что положительно скажется на росте цифровой безопасности.

Адекватное осознание объемов угроз цифровизации региональными властями позволяет выстраивать грамотную политику регулирования, защиты и развития цифровой трансформации всех сфер. Региональному Правительству важно формировать долгосрочные стратегии, которые обеспечат баланс между цифровой трансформацией и безопасностью и технологическим суверенитетом страны в целом.

Литература

1. Шевченко О.М. Цифровое неравенство в современном российском обществе: уровни и социальные последствия // Гуманитарий Юга России. 2023. № 1. С. 54-65.

2. Лялькова Е.Е., Богдашкина Е.А., Лобкова В.Э. Влияние искусственного интеллекта на рынок труда: анализ изменений в спросе на квалификации и обучении// E-Scio. 2023. № 5 (80). [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/vliyanie-iskusstvennogo-intellekta-na-rynok-truda-analiz-izmeneniy-v-sprose-na-kvalifikatsii-i-obuchenii (дата обращения: 11.06.2025).

3. Дубень А.К. Новые вызовы и угрозы в цифровом пространстве: безопасность как критерий развития информационных технологий// Вопросы безопасности. 2023. № 3. С. 11-20.

4. Ермакова О.М. Влияние ситуации изоляции на психическое здоровье людей// Ученые записки Санкт-Петербургского университета технологий управления и экономики. 2021. № 2 (74). С. 52-59.

5. Русакова О.И., Головань С.А. Анализ кибербезопасности в контексте современных угроз // Управленческий учет. 2022. № 10-2. С. 496-504.

6. Козырева С.Е., Яковлева Н.В. Киберпреступность как новейшая разновидность теневой экономики РФ // Международный журнал гуманитарных и естественных наук. 2023. № 6-1 (81). С. 70-73.

7. ФСБ: на Украине действует до 150 колл-центров, занятых мошенничеством. Сетевое издание «Коммерсантъ». [Электронный ресурс]. URL: https://www.kommersant.ru/doc/7710962 (дата обращения: 05.07.2025).

8. Синица С.А. Киберугрозы цифровой экономике России// Экономика и бизнес: теория и практика. 2023. № 11-3 (105). С. 65-70.

9. Хакеры усилили давление на критическую информационную инфраструктуру России – исследование. Информационное агентство «КомпРАС». [Электронный ресурс]. URL: https://compras.ru/hakery-usilili-davlenie-na-kriticheskuju-informacionnuju-infrastrukturu-rossii-issledovanie (дата обращения: 01.07.2025).

10. Аналитика МТС RED: около половины атак на промышленные предприятия совершается в нерабочее время. [Электронный ресурс]. URL: https://mobile-review.com/all/press_releases/analitika-mts-red-okolo-poloviny-atak-na-promyshlennye-predpriyatiya-sovershaetsya-v-nerabochee-vremya/(дата обращения: 01.07.2025).

11. Бородавко Л.С. Экономическая безопасность Российской Федерации в условиях санкционного давления // Финансовая экономика. 2024. № 11. С. 113-120.

12. Реестр открытых данных. Единая межведомственная информационно-статистическая система (ЕМИСС). [Электронный ресурс]. URL: https://www.fedstat.ru/opendata/7708234640-fiveanineaeightafiveatwo (дата обращения: 01.07.2025).

13. Об использовании информационных технологий населением Иркутской области. Официальный сайт «Иркутскстат». [Электронный ресурс]. URL: https://38.rosstat.gov.ru/storage/mediabank/ИКТ%20НАСЕЛЕНИЯ%202024.pdf (дата обращения: 01.07.2025).

14. Использование сети интернет. Официальный сайт «Крымстат». [Электронный ресурс]. URL: https://82.rosstat.gov.ru/storage/mediabank/1-ИАМ%20ИКТ%202024.pdf (дата обращения: 01.07.2025).

15. Сольская И.Ю., Русакова О.И., Меркулов А.С. и др. Инфраструктурные аспекты управления социально-экономическими системами. Иркутск: Иркутский государственный университет путей сообщения, 2022. 310 с.

16. Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств. Официальный сайт Банка России. [Электронный ресурс]. URL: https://cbr.ru/statistics/ib/review_3q_2024/(дата обращения: 01.07.2025).

17. Доступность финансовых услуг для жителей иркутской области. Официальный сайт Правительства Иркутской области. [Электронный ресурс]. URL: https://irkobl.ru/sites/digital/1_ЦБ.pdf (дата обращения: 01.07.2025).

18. Постановление Правительства Иркутской области от 13 ноября 2023 года № 1020-пп «Об утверждении государственной программы Иркутской области «Цифровое развитие, связь и телекоммуникации»». Официальный сайт Правительства Иркутской области. [Электронный ресурс]. URL: https://irkobl.ru/sites/digital/realizgpsprog/1020-пп%20(ГП).pdf?ysclid=mcq92ko8nu504428300 (дата обращения: 01.07.2025).