**УДК 338.43 DOI: 10.14451/1.232.121**

# Обеспечение экономической безопасности в эпоху цифровой экономики

© 2024 **Горбатко Елена Самратовна**
Кандидат экономических наук, доцент кафедры финансов, бухгалтерского учета и экономической безопасности. Московский государственный университет технологий и управления им. К. Г. Разумовского (Первый казачий университет), Россия, Москва.
E-mail: e.horbatko@mgutm.ru

© 2024 **Корнева Галина Викторовна**
Кандидат экономических наук, доцент кафедры финансов, бухгалтерского учета и экономической безопасности, Московский государственный университет технологий и управления им. К. Г. Разумовского (Первый казачий университет), Россия, Москва.
E-mail: g.korneva@mgutm.ru

© 2024 **Смирнова Анастасия Константиновна**
Магистрант кафедры финансов, бухгалтерского учета и экономической безопасности. Московский государственный университет технологий и управления им. К. Г. Разумовского (Первый казачий университет), Россия, Москва.
E-mail: a_smirnova@list.ru

Ключевые слова: цифровая экономика, экономическая безопасность, киберугрозы, меры безопасности, предотвращение кибератак, цифровая среда, угрозы, цифровизация.

Цифровая экономика становится все более важной для развития страны. Тем не менее, рост цифровых технологий также приносит новые угрозы. Кибератаки могут привести к серьезным последствиям для экономики и финансовой системы. Для обеспечения безопасности необходимо внедрять эффективные меры защиты от киберугроз. Только таким образом можно сохранить стабильность цифровой экономики и предотвратить серьезные угрозы для бизнеса и граждан. Также необходимо усилить защиту персональных данных и кибербезопасность. Важно развивать кадровый потенциал в области цифровой экономики, повышать квалификацию специалистов и привлекать талантливых IT-специалистов. Укрепление международного сотрудничества и обмен опытом также играют важную роль в обеспечении экономической безопасности в цифровой эпохе. Все вышеперечисленные меры помогут минимизировать угрозы и риски, сопутствующие росту цифровой экономики, и обеспечат устойчивое развитие страны в цифровую эру.

Цифровизация непрерывно трансформирует общество, фундаментально изменяя политические, социальные и экономические механизмы. Это стимулирует расширение предпринимательских инноваций, производительности и региональный экономический рост. Современная эконо-

мическая наука стоит на пороге формирования новой парадигмы, отражающей современные реалии комплексного использования информационных технологий, влияние которых привело к формированию новой экономической системы.

Результаты исследований по всему миру показывают, что в настоящее время в экономической науке не существует общепринятого определения цифровой экономики, а различные ученые и исследователи выдвигают выявленные основные черты цифровой экономики в предлагаемых ими теориях [4]. Сегодня возрастающая роль информации и внедрение коммуникационных технологий в производство привели к формированию информированного общества, основанного на нематериальных, интеллектуальных ресурсах: информации, знаниях, науке и человеческом капитале, а не на традиционных материальных. Первые исследования в области информации начались в 1940 году в рамках только что зародившейся науки — кибернетики. Хотя К. Шеннон в своих исследованиях теории коммуникации ограничился анализом ее количественных и технических свойств, он заложил основу для развития теории информации. Н. Винеп дал научное определение категории «информация», характеризуя ее как общенаучное, а не специфическое понятие. Следует отметить, что до сих пор в изучении информации доминирует технократический подход, который сужает ее важные содержательные характеристики и оценку ее роли в общественном развитии. В определенной степени это ограничение преодолевается за счет использования различных научных подходов к ее интерпретации в современной теории информации. Ученые напрямую связывают возникновение нового типа экономики с понятием информационного общества. Распространение сети интернет с широким охватом в период с 1996 по 2007 год оказало экономически значимый и устойчивый эффект, который позволил повысить годовой рост ВВП на душу населения [1].

Цифровизация также имеет последствия для глобальных экономических трансформаций, рынка труда и политического участия. И это предъявляет новые требования к уровню образования и подготовке кадров в экономическом секторе, а также заставляет разрабатывать новые меры по обеспечению экономической безопасности в цифровой экономике. Исследование экономической кибербезопасности актуально в связи с усилением конкуренции на мировом рынке и военными конфликтами, которые становятся важнейшими вопросами для государства. Изучение экономической кибербезопасности позволяет выявить проблемные аспекты экономики страны, найти решения и разработать стратегии обеспечения устойчивой инвестиционной политики. Наиболее значимые цифровые изменения затрагивают экономическую безопасность, поскольку высокая открытость компаний способствует возникновению различных угроз и рисков для их деятельности. Создание системы безопасности, которая будет отвечать всем тенденциям и изменениям, происходящим в цифровых социально-экономических процессах, является важной и актуальной задачей национальной экономики.

«Прогнозирование угроз и вызовов — ключевая задача в обеспечении экономической безопасности. Глобальным вызовом современности является цифровая трансформация. Цифровизация техносферы играет важную роль в научной, социальной и экономической сферах. Ведущие цифровые державы, такие как США, Китай и Япония, сильно зависят от цифровых технологий для развития своей экономики» [9]. Ежегодно в России выделяются миллиарды на развитие цифровой экономики и поддержание безопасности внутренних цифровых процессов. Это валовые внутренние затраты, которые превышают 3 миллиарда рублей ежегодно, включающие внутренние затраты организаций, а также затраты домашних хозяйств [1]. Расчёты за 2017 и 2018 года не учитывают затраты на цифровой контент.

«Правительство Российской Федерации разработало и утвердило Программу «Цифровая экономика в Российской Федерации» до 2035 года, которая включает вопросы, связанные с раз-

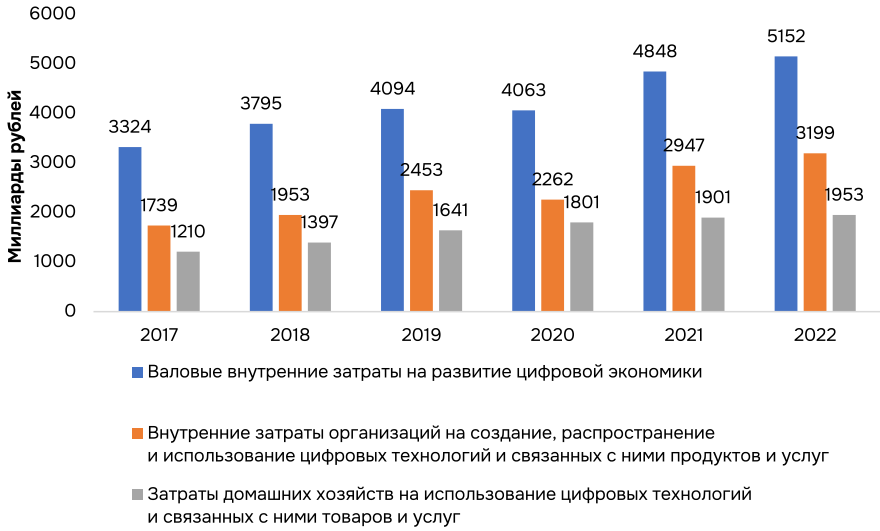


**Рис. 1.** Затраты на развитие цифровой экономики России [1].

работкой и внедрением технологий, анализом «больших данных» и прогнозированием, созданием новых способов управления и т. д. Данная программа должна решить одну из задач стратегического значения — сохранение суверенитета на фоне глобализации и реализацию программ цифрового развития с другими участниками мирового рынка» [5]. За последние несколько лет возросла необходимость в разработке мер по обеспечению безопасности цифровой экономики, поэтому большая часть бюджетов уходит не только на созидание, но и на сохранение и создание системы защиты. Всё чаще происходят инциденты со взломом, кражей и неправомерным использованием данных, связанных с финансами. Кибератаки представляют собой постоянную угрозу во всем мире как для правительств, компаний, так и для частных лиц. Публичное признание факта взлома обычно влечет за собой значительный репутационный ущерб в дополнение к потерям из-за кражи данных и интеллектуальной собственности, а также повреждения систем. Исследования по всему миру показывают, что количество кибератак увеличивается из года в год в геометрической прогрессии.

В сегодняшних реалиях не возникает вопроса, представляют ли кибератаки угрозу финансовой стабильности и могут ли они произойти, угроза от кибератак уже является реальностью и одним из важнейших вопросов на повестке дня в рамках обеспечения безопасности цифровой экономики. Тем не менее, правительства и компании всего мира продолжают изо всех сил пытаться сдерживать угрозы, даже когда остается неясным какие масштабы может принять кибератака, специалисты стараются предугадать варианты угроз и создать наиболее эффективную защиту системы. Все больше обеспокоенных ключевых фигур в экономике и других областях бьют тревогу, кибербезопасность волнует все страны мира. Уже в феврале 2020 года Кристин Лагард, президент Европейского центрального банка и бывший глава Международного валютного фонда, предупредила, что кибератака может спровоцировать серьезный финансовый кризис [5]. Уже давно стало понятно, что крупный киберинцидент, если его не пресечь должным образом, может серьезно подорвать финансовые системы, включая критически важную финансовую инфраструктуру, что приведет к более широким последствиям для финансовой стабильности. Потенциальные экономические издержки таких событий могут быть огромными, а ущерб общественного доверия к власти, всем финансовым инструментам, которые рекомендованы населению — значительным.

Две текущие тенденции усугубляют этот риск.

Во-первых, мировая финансовая система переживает беспрецедентную цифровую трансформацию, которую значительно ускорила прошедшая пандемия COVID-19. Цифровые технологии разрушили устаревшие системы общественной безопасности, которые зачастую не подходят для защиты от кибератак. Правовые и политические реформы, а также мероприятия по их реализации необходимы в каждой стране для решения постоянно растущих проблем кибербезопасности. Центральные банки по всему миру рассматривают возможность поддерживать цифровые валюты и модернизировать платежные системы. И в такой период, когда учёба и работа переходят в онлайн-пространство, покупки совершаются в интернете по 1 клику, все данные физических лиц, компаний и даже важная государственная документация хранятся в цифре, обеспечение кибербезопасности становится важным как никогда. Например, сильным потрясением для россиян стало отключение платёжной системы SWIFT, которое дополнилось огромным количеством информации о краже личных данных российских пользователей. Во-вторых, злоумышленники пользуются этой цифровой трансформацией и представляют растущую угрозу глобальной финансовой системе, финансовой стабильности и уверенности в целостности системы. Cybersecurity Ventures ожидает, что глобальные расходы на киберпреступность будут расти на 15% в год в течение следующих пяти лет, достигнув 10,5 триллионов долларов США в год к 2025 году по сравнению с 3 триллионами долларов США в 2015 году. Это представляет собой крупнейшую передачу экономического богатства в истории, ставит под угрозу стимулы для инноваций и инвестиций, экспоненциально превышает ущерб, нанесенный стихийными бедствиями за год, и будет более прибыльным, чем глобальная торговля всеми основными незаконными наркотиками вместе взятыми [6]. Хотя многие субъекты угроз сосредоточены на зарабатывании денег, количество направленных исключительно на разрушение атак растет. Более того, те, кто привык просто воровать, также узнают о сетях и операциях финансовой системы, что позволяет им совершать более разрушительные и масштабные атаки, а также в будущем продавать такие знания и возможности другим. Такая быстрая эволюция картины рисков усложняет реагирование даже зрелой и хорошо регулируемой системы.

Позиция России в отношении киберпреступности неоднозначна и сложна. Хотя российское правительство, похоже, борется с киберпреступностью и демонстрирует сильную волю к регулированию криптовалют (которые также используются киберпреступниками для обхода существующих банковских правил), оно также может иметь связи с хакерскими группами, чтобы преследовать свои собственные цели в цифровом экономическом поле. В цифровой экономике полное устранение опасности или риска неизбежно влечет за собой отказ от дополнительных возможностей экономического развития и на данный момент не представляется возможным.

В России за последние годы масштабы финансовой киберпреступности значительно расширились. Однако трудно определить точное количество групп, действующих в России, поскольку они легко скрываются, переформировываются, уходят в тень и потом восстанавливаются. Сообщество киберпреступников в России использует онлайн-платформы для проведения вредоносных операций для общения, продвижения или даже продажи «услуг» и «продуктов», в результате которых происходит отмывание и конфискация денежных средств. В зависимости от типа и размера преступной группы руководители группировок либо нанимают «сотрудников» для выплаты им фиксированной зарплаты, либо временно работают с ними на внештатной основе, привлекая для выполнения каких-то конкретных задач. В этих группировках незаменимы «денежные мулы»: их используют для перевода украденных денег на хакерские счета. Киберпреступные группы в основном используют криптовалюты для ведения своей незаконной деятельности. Одним из средств пресечения стало отключение в России крупнейших сервисов по работе с криптовалютой. Киберпреступность, рассматрива-

емая в рамках экономической системы, — это особый вид человеческой деятельности, направленный на поиск пробелов в правилах и моделях функционирования экономических механизмов, в методах экономической деятельности, в методах контроля экономической деятельности, а также в уголовном праве, в практике правоохранительных органов и органов юстиции [2]. Важной чертой является то, что цифровое финансовое мошенничество имеет характеристики, которые отличают его от других видов преступлений и одним из наиболее актуальных вопросов является тот факт, что данный вид преступлений совершается в кредитно-финансовой сфере, что наносит значительный ущерб экономике. Программы-вымогатели — вредоносное программное обеспечение, которое заражает компьютеры и мобильные устройства, и ограничивает их доступ к файлам, часто угрожая безвозвратным уничтожением данных, если не будет уплачен выкуп, — достигло масштабов эпидемии во всем мире и является одним из самых популярных методов атаки для киберпреступников.

Формирование необходимых социально-экономических условий способствует ускорению форм цифровизации экономики на всех уровнях, что является приоритетным условием обеспечения экономической безопасности государства. Сегодня цифровизация является одним из основных факторов развития мировой экономики, поскольку она не только повышает производительность труда (прямое преимущество), но и экономит время, создает новый спрос на новые товары и услуги, новое качество и ценность (косвенное преимущество) и т. д. В то же время использование цифровой информации как ресурса генерации обуславливает переход от традиционной рыночной экономики к цифровой экономике, в которой все секторы взаимосвязаны. Учитывая свою роль в экономике, финансовые учреждения необходимы для обеспечения ликвидности, гарантии безопасности денежной массы в экономике, предоставления кредитов, сбережений и депозитов, а также для обеспечения осуществления платежей и расчетов, что стало труднее сохранять в полной безопасности с быстрыми темпами цифровизации. Финансовые институты являются основой экономики. В связи с этим последнее влияние кибератак на финансовые учреждения может иметь очень серьезные последствия [5]. Экономическая безопасность должна быть выстроена таким образом, что вся институциональная система будет способна в полной мере отражать атаки, защищать интересы хозяйствующих субъектов, при этом бесперебойно функционируя и базируясь на национальных и международных правовых нормах. Создание такой структуры позволит обеспечивать стабильность экономики, бизнес-процессов, поддерживать экономический рост и снижать уровень экономических рисков.

В современных условиях только при своевременном прогнозировании потенциальных вызовов, а также определении скорости и вектора движения цифровой трансформации, можно добиться относительной стабильности и безопасности процессов цифровой экономики. На наш взгляд, для обеспечения экономической безопасности и дальнейшего позитивного развития государства в сферах цифровой экономики должна быть разработана специальная программа развития цифровой экономики, в которой будут выделены приоритетные направления. Трудно разработать такую систему безопасности, которой будет возможно эффективно управлять и быстро изменять, подстраивая под новые угрозы, если нет точных данных о том, что и от кого необходимо защитить. Поэтому для построения эффективной системы безопасности должна работать разветвленная информационная инфраструктура, позволяющая получать своевременный и безопасный доступ к информации [3]. В первую очередь должно быть качественно разработанное нормативное регулирование цифровой отрасли, которое будет стартом для формирования нового подхода к выявлению необходимых законодательных ограничений в отрасли. Вторым этапом идёт повышение цифровой грамотности населения страны (в том числе достижение высоких показателей выпуска компетентных специалистов

в области ИКТ). Параллельно с обучением идёт создание конкурентных условий для формирования в регионах крупных, средних и малых предприятий, работающих в сфере цифровых технологий, и вывода ряда этих компаний на международные рынки. Обеспечение населения страны доступом к широкополосному интернету, развитие новых технологий и средств связи (в том числе для формирования технологической основы функционирования системы связи на основе отечественных разработок). Казалось бы, что уже все обеспечены быстрым интернетом, он доступен в каждом городе, но всё ещё остаются обширные территории с плотным населением, где есть проблемы с доступом к цифровым технологиям. Программа должна быть тщательно разработана с учётом обеспечения уровня экономической безопасности страны, помимо вышеперечисленных направлений. Одной из целей программы развития цифровой экономики является обеспечение информационной безопасности. Ежемесячно программисты обнаруживают около 12 миллионов новых вредоносных программ.

Российская ассоциация электронных коммуникаций (РАЭК) отмечает: «Крайне важно поддерживать международный диалог в сфере кибербезопасности: на уровне государственной политики необходимо поддерживать баланс между обеспечением национальной безопасности и сохранением трансграничного и глобального характера инфраструктур» [7]. Чтобы подготовиться к цифровым экономическим угрозам, создаются локальные организованные группы реагирования на инциденты компьютерной безопасности. Для координации превентивных мер и реагирования на инциденты на территории страны действуют специалисты в сфере ИКТ с конкретными обязанностями в области кибербезопасности.

На сегодняшний день создан сайт «Дайджест цифровой экономики», на котором представлены ключевые исследования и публикации по цифровой экономике и цифровым технологиям в России и в мире. Основными причинами возникновения рисков и угроз экономической безопасности являются неразвитость институциональных основ общества, дисбаланс формальных и неформальных институтов, их низкая эффективность. В настоящее время специалисты по безопасности, как правило, уделяют особое внимание защите конфиденциальности, целостности и доступности критически важной информации, а также обеспечению подотчетности. Нет сомнений в том, что успех цифровой экономики во многом зависит от степени безопасности механизмов и инструментов, которые задействованы в работе. В связи с этим возникает крайняя необходимость в формировании инструментов и навыков работников, которые позволят в короткий срок с наибольшей эффективностью внедрять изменения в информационную инфраструктуру. В первую очередь развитие должно быть направлено на человеческий ресурс, на образование и поддержание актуального уровня компетентности сотрудников. Несмотря на то, что цифровые технологии моделируют бизнес, процессы и управление в цифровой экономике, люди остаются ключевым ресурсом для реализации стратегии информационной безопасности.

Функционирование цифровой экономики зависит от тесного взаимного сотрудничества различных основных системных элементов. Данные, как ключевой производственный фактор, приобретают свою ценность не обособленно, а, скорее, благодаря сложной связи с физическими носителями, такими как процессоры данных и устройства хранения данных. В общей цифровой экономической модели накопление данных ограничено возможностями хранения данных, а эффективность использования данных зависит от вычислительной мощности конкурентов. Когда данные распределяются и используются без конкуренции во всех секторах производства и инноваций, объем генерируемых данных, общая вычислительная мощность и распределение вычислительных ресурсов взаимно влияют друг на друга, что приводит к равновесию рыночной конкуренции. Однако это равновесие может привести к потенциальным проблемам, таким

как чрезмерные инвестиции в вычислительные мощности, неравномерное распределение вычислительных ресурсов и недостаточность инноваций во время рыночной конкуренции. Более того, при различных настройках параметров рыночное конкурентное равновесие может испытывать неадекватный обмен данными или неправильное использование данных.

**Библиографический список**


1. *Дудин М. Н., Шкодинский С. В.* Вызовы и угрозы цифровой экономики для устойчивости национальной банковской системы. Финансы: теория и практика // Finance: Theory and Practice. — 2022. — 26 (6). — С. 52—71. — DOI: 10.26794/2587-5671-2022-26-6-52-71.
2. *Мамателашвили О. и Кулагина З. Д.* Экономическая безопасность бизнеса в цифровой экономике // Экономические и социальные тенденции устойчивого развития современного общества (ICEST-II 2021), том 116. Европейские труды социальных и поведенческих наук / И. В. Ковалев, А. А. Ворошилова, А. С. Будагов. — Европейское издательство, 2021. — С. 878—887. — DOI: 10.15405/epsbs.2021.09.02.99.
3. *Манахова И. В.* Цифровое будущее и глобальная экономическая безопасность // Экономическая безопасность и качество. — 2018. — 1 (30). — URL: http://www.seun.ru/content/nauka/5/1/doc/Economical%20security_1_30_2018.pdf.
4. *Отакузиева З. М.* Формирование информационной экономики: перспективы ее формирования и перспективы ее развития в Узбекистане // Научный вестник. — 2016. — 1(7). — С. 107—113.
5. Правительство Российской Федерации / Развитие цифровой экономики в России. Программа до 2035 года (№ 1632-р). — 2017.
6. *Стрижов С. А.* Барьеры и риски цифровой экономики. Инновации. Инвестиции (118) УЭкС, 12/2018 / Институт бизнеса и делового администрирования Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации. — URL: http://uecs.ru/index.php?option=com_flexicontent&view=items&id=5330.
7. Указ Президента Российской Федерации от 13.05.2017 г. № 208 «О стратегии экономической безопасности Российской Федерации на период до 2030 года». — URL: http://www.kremlin.ru/acts/bank/41921.
8. Цифровая экономика РФ: экспертное мнение / Финам. — 2017. — URL: https://www.finam.ru/analysis/forecasts/cifrovaya-ekonomika-rf-ekspertnoe-mnenie-20170705-170347.
9. Цифровая экономика: 2024: краткий статистический сборник / В. Л. Абашкин [и др.]. — М. : ИСИЭЗ ВШЭ, 2024.