

**Ссылка для цитирования этой статьи:**

Гирфанова И.Н., Имамова К.Р., Пруденко А.Н. Экономика цифровой безопасности // Human Progress. 2024. Том 10, Вып. 5. URL: [http://progress-human.com/images/2024/Tom10\\_5/Girfanova.pdf](http://progress-human.com/images/2024/Tom10_5/Girfanova.pdf) DOI 10.46320/2073-4506-2024-5a-8.

## ЭКОНОМИКА ЦИФРОВОЙ БЕЗОПАСНОСТИ

**Гирфанова Ирина Насхетдиновна**

кандидат экономических наук, доцент  
Башкирский государственный аграрный университет  
г. Уфа, Российская Федерация

**Имамова Карина Руслановна**

магистрант Института истории и государственного управления  
Уфимского университета науки и техники  
г. Уфа, Российская Федерация

**Пруденко Артем Николаевич**

магистрант Института истории и государственного управления  
Уфимского университета науки и техники  
г. Уфа, Российская Федерация

**Аннотация.** Цифровая безопасность – ключевой аспект развития современной национальной экономики, обеспечивающий устойчивое развитие всей национальной экономики в современной цифровой среде. Объект исследования – цифровая экономика. Предмет исследования – безопасность, как состояние экономической системы. Цель исследования – рассмотреть экономику цифровой безопасности как состояние национальной экономики, обеспечивающее устойчивой развитие. В данном исследовании подчеркивается важность цифровой безопасности в контексте современного все более цифрового мира, обсуждается несколько ключевых вопросов и подчеркивается значение цифровой безопасности для различных аспектов функционирования общества, включая его экономическое развитие. Подчеркивается что национальная экономика проходит этап цифровой трансформации, вызванной цифровизацией и внедрением цифровых технологий в различных секторах экономики. С цифровым прогрессом экономики появляются растущие проблемы, создаваемые киберугрозами, включая кибератаки и кибермошенничество и в этом контексте подчёркивается важность понимания последствий кибератак и внедрения надежных мер кибербезопасности имеет первостепенное значение.

**Ключевые слова:** цифровая экономика, киберугрозы, устойчивое развитие, цифровая трансформация, цифровизация.

## **Введение**

Цифровая безопасность представляет собой комплексный подход к обеспечению безопасности во всех цифровых средах, в которых взаимодействуют экономические агенты. Более широко известная как цифровая безопасность, она охватывает все устройства с доступом к интернету, от ноутбуков до смартфонов, формируя защиту инфраструктуры и коммуникаций. Цифровая безопасность предполагает наличия осознания потенциальных угроз, возникающих при активном использовании интернета, включая в себя управление и защиту личных данных, меры предосторожности против угроз безопасности, а также избегание нелегального контента. Обеспечение цифровой безопасности означает защиту мобильных устройств, ноутбуков, планшетов и других подключенных к интернету устройств от потенциальных злоумышленников или угроз, таких как фишинг или взлом.

Существует множество способов обеспечить собственную безопасность в сети, от двухфакторной аутентификации до использования VPN, то есть цифровая безопасность - это набор процессов и технологий, разработанных для защиты устройств и сетей от атак, несанкционированного доступа или повреждений. В современном цифровом мире, где данные являются краеугольным камнем любой коммерческой деятельности, кибербезопасность стала неотъемлемой частью работы многих корпораций и организаций по всему миру, когда утечка данных может привести к серьезным негативным последствиям. Кибербезопасность, как правило, защищает все типы данных от повреждения или кражи, обеспечивая более адаптивную цифровую жизнь.

## **Методология исследования**

Термин «цифровая экономика» описывает новые формы бизнеса, рынки, продукты и услуги, основанные на использовании цифровых технологий как ключевого элемента инфраструктуры всего современного хозяйствования. Концепция цифровой экономики базируется на объединении и одновременном использовании различных цифровых технологий, которые были созданы отдельно, но теперь доступны для совместного применения. Ее также можно определить как комбинацию информационных, вычислительных, коммуникационных и сетевых технологий: «Перечисленные обстоятельства, а также целый ряд других обстоятельств, связанных с процессами цифровизации в общемировом масштабе, влекут за собой необходимость разработки адаптивных стратегий и подходов, учитывающих эти вызовы и позволяющих обеспечить

стабильность, устойчивость и социальное благополучие в долгосрочной перспективе» [1, с. 68].

Экспоненциальный прогресс в соотношении цены и производительности вычислений, хранения, пропускной способности и программных приложений открывает путь к следующему поколению цифровых технологий, предоставляемых через облачные сервисы: «Как показывают исследования, большинство нарушений безопасности происходят из-за человеческого фактора (небрежности при обращении с данными или недостаточной осведомленности о методах защиты)» [2, с. 98].

Кибератаки, связанные с экономическим противостоянием, стали серьезной угрозой для бизнеса и часто приводят к финансовым потерям, так как в последние годы наблюдается рост числа предприятий по всему миру, внедряющих искусственный интеллект в свою деятельность. ИИ помогает компаниям снижать операционные расходы, повышать производительность и улучшать обслуживание клиентов, то есть национальная экономика получила преимущества не только от доступа к новым рынкам, но и от свободного потока информации, который стал возможен благодаря развитию информационных технологий и интернета: «Теперь уровень экономической безопасности страны определяется уровнем развития цифровых технологий в экономике страны» [3, с. 71].

Бизнес процветает в новой экономике благодаря доступности своевременной информации и свободного обмена знаниями, что помогает оптимизировать процессы принятия решений и создавать индивидуальные товары и услуги, удовлетворяющие конкретные потребности клиентов, то есть информационные технологии значительно изменили способ ведения бизнеса в современную эпоху. Бизнес может лучше планировать инвестиции и управление запасами, а также сокращать расходы на рекламу и маркетинг благодаря расширенному доступу к информации, но экономика цифровой безопасности выступает ключевым направлением устойчивости развития бизнеса [4].

Вопрос кибербезопасности активно обсуждается как в академических, так и в популярных изданиях, однако большинство работ придерживаются единого, часто неполного представления о предмете. Термин «кибербезопасность» употребляется слишком широко, и его определения зависят от контекста, часто субъективны и неинформативны. Отсутствует единое определение, которое бы отражало многогранность кибербезопасности, что затрудняет технологический и научный прогресс. Нечеткое определение способствует техническому взгляду на кибербезопасность и разделяет различные дисциплины, которые должны работать вместе для решения сложных проблем, мало того, само понимание цифровой экономики не имеет единого определения и единого подхода к решению проблем: «Формирующаяся

цифровая экономика обладает потенциалом для новых научных исследований и открытий, создания рабочих мест и экономического роста. Сегодня на всей нашей планете нет согласованного мнения о таком явлении, как «цифровая» экономика, но есть множество определений» [5, с. 48].

Существует широкий спектр технических решений для обеспечения кибербезопасности, но этого недостаточно для решения проблемы в целом: существуют исследования, демонстрирующие важность организационных, экономических, социальных, политических и других факторов, которые тесно связаны с кибербезопасностью, но они фрагментарны и не представляют собой цельный комплекс решений.

### **Результаты исследования**

Цифровая безопасность - это метод защиты инфраструктуры цифровой экономики, сетей и программ от цифровых атак. Цифровые атаки обычно преследуют три цели: получение доступа к конфиденциальной информации, изменение или удаление этой информации, вымогательство денег (например, с помощью программ-вымогателей) или нарушение нормальной деятельности компании.

Цифровую безопасность также можно определить как набор технологий, процедур, практик, мер реагирования и методов смягчения последствий, направленных на защиту сетей, компьютеров, программ и данных от атак, повреждений или несанкционированного доступа. Цель - обеспечить конфиденциальность, целостность и доступность информации.

Рост цифровизации и цифрового бизнеса создает множество возможностей для быстрого развития новых возможностей и получения конкурентного преимущества, когда цифровая экономика предлагает удобство круглосуточных услуг, доступных из дома.

Использование цифровых решений и новых технологий может помочь решить основные проблемы развития и обеспечить доступ ко всем бизнес-услугам для всех. Бизнесу необходимо идти в ногу с цифровой революцией, чтобы сохранять конкурентные преимущества и устойчивость на рынке, но использование больших данных и цифровых систем, доступных через интернет и различные ИТ-устройства, может поставить под угрозу способность компании защищать свою конфиденциальность.

После глубокого анализа различных определений цифровой безопасности авторы пришли к комплексному определению, определив ее как организацию и совокупность ресурсов, процессов и структур, призванных защищать киберпространство и работающие в нем системы от событий, нарушающих юридические и фактические права собственности, что может произойти, когда юридические права собственности не соответствуют фактическим.

Экономика является краеугольным камнем человеческого общества, являясь основой нашего существования, так как организует распределение ресурсов, производство основных товаров и услуг, а также их потребление, обеспечивая наше выживание. Этот сложный институт включает в себя множество видов деятельности, имеющих решающее значение для развития и прогресса наций и решения, принимаемые в рамках этого института, влияют на благосостояние людей, подчеркивая его значимость.

За последние десятилетия экономический ландшафт претерпел глубокие изменения и продолжает развиваться. Внедрение цифровых технологий в деятельность постиндустриальных обществ подтверждает эту реальность, так развивающиеся экономики быстро сокращают разрыв с более развитыми странами, используя цифровые инструменты для управления своей экономикой и важно отметить, что даже в сельской местности цифровые технологии преобразуют повседневные бизнес - операции.

Подобная эволюция подчеркивает необходимость в строгих мерах кибербезопасности для защиты киберпространства. Обеспечение безопасности киберпространства имеет решающее значение не только для использования всех преимуществ цифровых технологий, но и для предотвращения потенциальных потерь, вызванных кибератаками, угрозами и мошенническими действиями.

Концепции цифрового развития разнообразны и многочисленны, отражая многогранность этого явления и точки зрения разных авторов и философов, с этой точки зрения (комплексной и системной) авторы воспринимают цифровое развитие как непрерывный процесс, направленный на улучшение всех аспектов общества с целью повышения качества жизни людей, что включает в себя экономическое благосостояние, политическую стабильность, образование, здравоохранение, судебную систему и даже религиозные аспекты.

Цифровое развитие - это многомерный процесс, предполагающий изменения в социальных структурах, общественных установках и национальных институтах. Он также включает в себя ускорение экономического роста, сокращение неравенства и искоренение бедности, но развитие не тождественно полной свободе от различных ограничений, цифровое развитие позволяет людям оперировать большим благополучием и автономией в выборе своего жизненного пути.

Цифровое развитие тождественно экономическому развитию - это устойчивое возвышение всего общества и его социальной системы к более устойчивому состоянию. В этом контексте становится очевидным, что цифровая безопасность играет ключевую роль в устойчивом развитии. По мере усиления цифровизации экономики, подобно более развитым

странам, необходимо уделять первостепенное внимание безопасности информационных систем в государственных учреждениях, особенно в свете растущей угрозы кибератак.

Уязвимая система цифровой безопасности, без сомнения, является одним из самых быстрых способов помешать развитию, учитывая значительные потери, которые она часто влечет за собой. В банковском секторе кибератаки на финансовые учреждения привели к существенным финансовым потерям. Киберпреступники постоянно ищут способы взломать информационные системы, получить доступ к данным о владельцах счетов и использовать их в мошеннических целях. Учебные заведения также стали жертвами утечек данных, когда хакеры незаконно получают доступ к личной информации сотрудников и студентов для мошенничества.

Несмотря на потенциальные потери, цифровизацию экономики необходимо поощрять, но с необходимыми мерами предосторожности для обеспечения эффективной цифровой безопасности всех цифровых систем. В цифровом обществе все секторы экономики зависят от информации, которая является ключевым элементом их функционирования, поэтому обеспечение безопасности информационных систем имеет первостепенное значение, особенно в контексте многочисленных существующих угроз и проблем во многих развивающихся экономиках мира. Любая угроза кибербезопасности является дополнительным бременем, требующим немедленного внимания.

Общественная формация «цифровой эпохи» характеризуется стремительными изменениями, затрагивающими различные аспекты, такие как подключение, интеграция, управление цепочками поставок, модели и другие. Как прямое следствие, безопасность стала высокоприбыльным бизнесом, а защита важной информации, операций и профиля потребителя выходит за рамки физической безопасности. В результате необходимо переосмыслить значение термина «безопасность» и повысить устойчивость технологических систем. Инфраструктура информационных технологий и электрические системы являются неотъемлемой частью электроэнергетической системы - системы охватывают киберпространство, людей, физические системы и финансы. Существует три основные категории рисков: физические, внутренние и внешние, и киберопасности могут исходить с любого направления. Борьба с киберпреступностью и кибератаками, направленными на национальные сектора экономики, представляет собой значительные проблемы. Эти опасности можно только минимизировать, но не полностью устранить. Смягчение угроз требует значительных затрат как в финансовом плане, так и в плане усилий, а также приводит к простоям и экономическим и финансовым последствиям для всего сектора. Решение проблем кибербезопасности имеет решающее значение для устойчивого развития наций. В

следующих разделах будут рассмотрены потенциальные решения и стратегии для смягчения этих проблем и обеспечения безопасного и надежного развития общества в цифровую эпоху.

### **Заключение**

Анализ собранной информации показывает, что киберугрозы и атаки - реальная и очевидная проблема национальной экономики, которые существуют в различных формах, способных поставить под угрозу целостность информационных систем и тем самым нанести значительный ущерб жертвам, как отдельным лицам, так и корпоративным организациям. Последствия для развития экономики могут быть крайне неблагоприятны и делают бесполезными усилия по улучшению цифрового производства и предоставления услуг с использованием цифровых технологий. Цифровая уязвимость может привести к финансовым потерям, стагнации и потере возможностей в экономическом развитии и прогрессе в других сферах общества. Включение безопасности в киберпространство имеет жизненно важное значение для предотвращения компрометации, обеспечения защиты конфиденциальной информации и права на неприкосновенность частной жизни, предотвращения мошенничества и поддержания общей целостности систем информации, где бы они ни находились, таким образом, преимущества применения цифровых технологий для экономического развития будут полностью исчерпаны.

В этом исследовании подчеркивается важность цифровой безопасности в контексте нашего всё более масштабирующегося цифрового мира, обсуждается несколько ключевых вопросов и подчеркивается значение цифровой безопасности для различных аспектов общества, включая его экономическое развитие. Подчеркивается что национальная экономика проходит этап цифровой трансформации, вызванной цифровизацией и внедрением цифровых технологий в различных секторах экономики. С цифровым прогрессом экономики указываются растущие проблемы, создаваемые киберугрозами, включая кибератаки и кибермошенничество и в этом контексте подчёркивается важность понимания последствий кибератак и внедрения надежных мер кибербезопасности имеет первостепенное значение.

Кроме того, исследование подчеркивает важную роль цифровой безопасности в обеспечении как национальной, так и глобальной безопасности в нашем современном мире. Оно признает положительные и отрицательные последствия распространения технологий и подчеркивает рост «информационных» рисков. С ростом цифровой экономики исследование подчеркивает возможности, которые она предлагает, и важность внедрения цифровых решений для предприятий, чтобы оставаться конкурентоспособными.

Исследование проводит различие между информационной безопасностью и цифровой безопасностью, подчеркивает необходимость эффективных мер безопасности для борьбы с передовыми киберугрозами. Также удостоверяет важность осведомленности о цифровой безопасности, включая сотрудников, руководство и возможности инфраструктуры для эффективного решения проблем кибербезопасности. Кроме того, это исследование подчеркивает важность укрепления цифрового доверия в отношениях между клиентами и бизнесом и его роль в снижении рисков и обеспечении лояльности клиентов, связывая цифровую безопасность с развитием, подчеркивая, что уязвимая система цифровой безопасности может помешать процессу экономического развития, особенно в таких секторах, как финансы и образование.

### Список литературы

1. Улыбина Л.В., Белогорская А.Н. Методология моделирования состояния экономической безопасности в условиях цифровой трансформации экономики // Вестник Российского университета кооперации. 2024. № 1 (55). С. 67-71. EDN PIIYSS.
2. Миргородская М.Г., Аничкина О.А., Иванова С.С. Влияние цифровой экономики на экономическую безопасность предприятий // Инновационное развитие экономики. 2024. № 1 (79). С. 95-99. DOI 10.51832/222379842024195. EDN UIJMPK.
3. Свирина М.В. Цифровая экономика как основа экономической безопасности страны // Современная наука. 2021. № 5. С. 70-72. DOI 10.53039/2079-4401.2021.7.5.015. EDN EXEWCM.
4. Кузовкова Т.А., Салютин Т.Ю. Влияние нового технологического уклада на цифровую безопасность экономики // Методические вопросы преподавания инфокоммуникаций в высшей школе. 2022. Т. 11, № 3. С. 13-19. EDN MFAVUI.
5. Крутова Н.А., Крутов А.Н., Иванчина О.В. Развитие цифровой экономики, проблема безопасности: риски, перспективы // Вестник СамГУПС. 2021. № 3 (53). С. 47-57. EDN REQHXT.

## THE ECONOMICS OF DIGITAL SECURITY

**Girfanova Irina Naskhetdinovna**

Candidate of Economic Sciences, Associate Professor  
Bashkir State Agrarian University  
Ufa, Russian Federation

**Imamova Karina Ruslanovna**

Undergraduate student Institute of History and Public Administration  
Ufa Institute of Science and Technology



Ufa, Russian Federation  
**Rudenko Artyom Nikolaevich**  
Undergraduate student Institute of History and Public Administration  
Ufa Institute of Science and Technology  
Ufa, Russian Federation

**Abstract.** Digital security is a key aspect of the development of modern national economy, ensuring the sustainable development of the entire national economy in the modern digital environment. The object of the study is the digital economy. Subject of the study - security as a state of the economic system. The purpose of the study is to examine the digital security economy as a state of the national economy that ensures sustainable development. This study emphasizes the importance of digital security in the context of today's increasingly digital world, discussing several key issues and emphasizing the importance of digital security for various aspects of the functioning of society, including its economic development. It is emphasized that the national economy is undergoing a phase of digital transformation caused by digitalization and adoption of digital technologies in various sectors of the economy. With the digital progress of the economy comes increasing challenges posed by cyber threats, including cyber attacks and cyber fraud and in this context the importance of understanding the consequences of cyber attacks and implementing robust cyber security measures is emphasized.

**Key words:** digital economy, cyber threats, sustainable development, digital transformation, digitalization.

#### References

1. Ulybina L.V., Belogorskaya A.N. Methodology of modeling the state of economic security in the context of digital transformation of the economy // Bulletin of the Russian University of Cooperation. 2024. № 1 (55). P. 67-71. EDN PIIYSS.
2. Mirgorodskaya M.G., Anichkina O.A., Ivanova S.S. The influence of the digital economy on the economic security of enterprises // Innovative development of the economy. 2024. № 1 (79). P. 95-99. DOI 10.51832/222379842024195. EDN UIJMPK.
3. Svirina M.V. Digital economy as the basis of the country's economic security // Modern science. 2021. № 5. P. 70-72. DOI 10.53039/2079-4401.2021.7.5.015. EDN EXEWCM.
4. Kuzovkova T.A., Salyutina T.Y. The impact of the new technological order on the digital security of the economy // Methodological issues of teaching infocommunications in higher education. 2022. Vol. 11, № 3. P. 13-19. EDN MFAVUI.
5. Krutova N.A., Krutov A.N., Ivanchina O.V. Development of the digital economy, the problem of security: risks, prospects // Bulletin of SamGUPS. 2021. № 3 (53). P. 47-57. EDN REQHXT.