Вестник Самарского государственного экономического университета. 2024. № 8 (238). С. 49–57.
Vestnik of Samara State University of Economics. 2024. No. 8 (238). Pp. 49–57.

Научная статья
УДК 004.8+004.62+338.46

# Информационная безопасность как важная составляющая цифровой экономики

**Кристина Олеговна Карлышева[1], Алина Рустемовна Булатова[2], Марат Исхакович Иваев[3]**
[1,2,3] Поволжский государственный университет телекоммуникаций и информатики, Самара, Россия
[1] Kristina.karlisheva@yandex.ru
[2] alinabulatova2002@yandex.ru
[3] ivaevmarat@yandex.ru

***Аннотация.*** В статье рассматриваются проблемы и значимость обеспечения безопасности информации в условиях цифровой экономики, способы защиты личных данных и концепция защиты информации. Цифровая экономика приводит к развитию всех сфер общественной жизни, однако сопровождается и угрозами потери конфиденциальных данных. Для обеспечения безопасности необходимо разработать эффективную систему информационной безопасности, включающую использование и развитие дополнительных информационных ресурсов. Одним из важных аспектов является формирование кадрового потенциала в области информационной безопасности через программы повышения квалификации. Переход к цифровой экономике является необходимым, однако обеспечение высокого уровня информационной безопасности выступает ключевым вопросом в этом процессе. В статье также выделены основы формирования информационного общества и цифровой экономики, проводится теоретический анализ основных понятий и признаков цифровой экономики, отличающих ее от других экономических моделей.

***Ключевые слова:*** информационная безопасность, информационные системы, безопасность, экономика, цифровая экономика, экономическая безопасность, угрозы экономической безопасности, национальная безопасность

***Основные положения:***

♦ цифровая экономика неразрывно связана с информационной безопасностью и является ключевым компонентом как для специалистов по безопасности, так и для всех участников процесса разработки и использования информационных технологий;

♦ цифровая экономика обладает рядом характерных признаков, отличающих ее от других экономических моделей;

♦ распространение цифровой экономики зависит от обеспечения информационной безопасности и защиты информационных систем от новых угроз.

***Для цитирования:*** Карлышева К.О., Булатова А.Р., Иваев М.И. Информационная безопасность как важная составляющая цифровой экономики // Вестник Самарского государственного экономического университета. 2024. № 8 (238). С. 49–57.

Original article

# Information security as an important component of the digital economy

**Kristina O. Karlysheva[1], Alina R. Bulatova[2], Marat I. Ivaev[3]**
[1,2,3] Volga Region State University of Telecommunications and Informatics, Samara, Russia
[1] Kristina.karlisheva@yandex.ru
[2] alinabulatova2002@yandex.ru
[3] ivaevmarat@yandex.ru

***Abstract.*** The article investigates problems and importance of ensuring information security in the digital economy, ways to protect personal data and the concept of information protection. The digital economy leads to the development of all spheres of public life, but it is also accompanied by threats of loss of confidential data. To ensure security, it is necessary to develop an effective information security system, including the use and development of additional information resources. One of the important aspects is the formation of human resources in the field of information security through professional development programs. The transition to a digital economy is necessary, but ensuring a high level of information security is a key issue in this process. The article also highlights foundations of the formation of the information society and the digital economy, and provides a theoretical analysis of the basic concepts and features of the digital economy that distinguish it from other economic models.

***Keywords:*** information security, information systems, security, economy, digital economy, economic security, threats to economic security, national security

***Highlights:***

♦ the digital economy is inextricably linked to information security and is a key component for both security professionals and all participants in the development and use of information technology;

♦ the digital economy has a number of characteristic features that distinguish it from other economic models;

♦ the spread of the digital economy depends on ensuring the information security and protecting information systems from new threats.

***For citation:*** Karlysheva K.O., Bulatova A.R., Ivaev M.I. Information security as an important component of the digital economy // Vestnik of Samara State University of Economics. 2024. No. 8 (238). Pp. 49–57. (In Russ.).

## Введение

Зарождение первых идей и концепций цифровой экономики произошло сравнительно недавно – в конце XX в. Многие ученые до сих пор не достигли консенсуса относительно определения цифровой экономики. Тем не менее большинство исследователей согласны с тем, что цифровая экономика представляет собой виртуальную среду, дополняющую реальность производственных отношений.

На одном из собраний Международной финансовой организации она была определена как модель ускоренного формирования экономики за счет использования современных цифровых технологий.

Существуют 2 системных подхода к пониманию сущности цифровой экономики как науки:

1) традиционный подход рассматривает цифровую экономику как экономику, которая основана на цифровых технологиях. Он акцентирует внимание на электронных товарах и услугах, таких как медиаконтент и образовательные онлайн-технологии;

2) углубленный подход определяет цифровую экономику как сектор финансов, который тесно взаимосвязан с применением цифровых технологий.

На сегодняшний день вместе с объемами увеличивается и диапазон повсеместного распространения области online-платежей, приме-

ром этому служат электронные платежные системы, продвижение криптовалют. Информационные технологические процессы заполняют все без исключения области социальной жизни людей. Эти технологии упрощают и стимулируют обмен информацией, а также значительно повышают производительность труда.

Одновременно с этим информатизация неминуемо влечет за собой киберриски, угрозы появления информационных опасностей, которые обусловливают необходимость более подробного изучения методов информационной безопасности [1].

Основные цели исследования:

1. Рассмотреть фундаментальные аспекты информационной безопасности и ее воздействие на цифровую экономику.

2. Изучить актуальные угрозы и риски, связанные с информационной безопасностью в цифровой среде.

3. Проанализировать меры и методы защиты информации в цифровой экономике.

4. Исследовать влияние нарушений информационной безопасности на экономическую деятельность организаций и государства в целом.

5. Предложить рекомендации по улучшению системы информационной безопасности в цифровой экономике.

В целом задача данной работы – оценка значимости информационной безопасности в цифровой экономике как инструмента ее стабильного функционирования, а именно:

1) дать характеристику информационной безопасности в конвенциях цифровизации экономики в контексте защиты государственных интересов Российской Федерации;

2) изложить и дать оценку результативности инструментов информационной защиты;

3) отметить основные тенденции государственной политической деятельности в сфере информационной безопасности цифровой экономики.

Научной новизной работы может быть исследование актуальных методов обеспечения информационной безопасности в цифровой экономике, анализ последних тенденций и вызовов в этой области, разработка новых подходов к защите данных и личной информации в онлайн-среде, исследование влияния угроз кибербезопасности на развитие цифровой экономики и другие оригинальные исследовательские результаты, которые могут дополнить существующие знания в этой области.

## Методы

Предметом исследования является информационная безопасность.

Гипотеза изучения включает в себя следующее: в условиях цифровизации экономики РФ национальная стратегия должна предусматривать новые угрозы информационной безопасности.

На национальном уровне информационная надежность/безопасность представляет собой меры, направленные на защиту интересов государства в информационной сфере, которая создается взаимодействием как государства, так и общества в целом.

На законодательном уровне информационная надежность определяется как состояние безопасности информационной сферы общества, позволяющее использовать данные в интересах страны, сообщества и индивида.

На уровне субъектов экономики информационная безопасность связана с защитой данных и инфраструктуры от негативного воздействия, включая владельцев и пользователей информации.

Вид информации воздействий может являться неожиданным или заранее запланированным, естественным или же искусственным.

Цифровая экономика имеет в своей основе 3 ключевых компонента:

1. Инфраструктура – это все те элементы, которые составляют основу цифровой экосистемы. Важным фактором является наличие современной аппаратуры и программного обеспечения, которые позволяют эффективно работать с цифровыми технологиями. Также в этот компонент входят телекоммуникационные устройства и другие средства связи, которые обеспечивают передачу данных и информации.

2. Электронный бизнес – это направление, связанное с использованием цифровых технологий для проведения коммерческой деятельности. Он включает в себя создание и управление веб-сайтами, онлайн-магазинами, электронными платформами для предоставления услуг и другими подобными решениями.

3. Электронная коммерция – это сфера, в которой осуществляется продажа товаров и услуг в режиме онлайн. Она позволяет потребителям приобретать нужные им продукты с помощью интернет-ресурсов, без необходимости физического посещения магазинов. Такие покупки удобны, доступны и дают возможность выбирать из широкого ассортимента товаров.

Все 3 элемента взаимосвязаны и являются неотъемлемой частью современной цифровой экономики, однако не охватывают суть происходящих процессов и не подчеркивают их взаимосвязь с новыми технологиями.

Исследование информационной безопасности как важной составляющей цифровой экономики предполагает использование различных методов анализа, оценки угроз, рисков и защиты информационных систем. Ниже приведены некоторые методы исследования, которые можно использовать при изучении данной темы:

♦ анализ рисков – помогает выявить возможные угрозы безопасности информации, а также оценить вероятность их возникновения и возможные последствия для цифровой экономики;

♦ исследование уязвимостей информационных систем – позволяет выявить слабые места, которые могут быть использованы злоумышленниками для атак. Такой анализ способствует разработке мер по устранению уязвимостей и повышению уровня безопасности;

♦ проведение аудита информационной безопасности – позволяет оценить соответствие информационной безопасности требованиям нормативных документов, стандартов и методологий;

♦ исследование технологий информационной безопасности – помогает определить эффективные способы защиты информации и инфраструктуры цифровой экономики;

♦ анализ законодательства и нормативных требований в области информационной безопасности – позволяет понять правовые аспекты защиты информации и осуществлять соответствующие действия для обеспечения безопасности данных.

Эти и другие методы исследования дают возможность получить глубокое понимание проблем информационной безопасности в контексте цифровой экономики и разработать эффективные стратегии и меры по ее защите.

Цифровая экономика представляет собой сферу экономической деятельности, в которой ключевым ресурсом являются цифровые данные. Обработка и массовое использование таких данных способствуют значительному увеличению производительности в различных отраслях производства и торговли [2; 3].

Данное определение не отражает некоторые протекающие процессы, но оно ближе к истине. Важно рассматривать цифровую экономику с учетом используемых технологий, которые лежат в ее основе и определяют качество происходящих изменений (табл. 1).

Новые информационные технологии содействуют расширению деловой сферы человека, а также его повседневных взаимодействий. В современной экономике информационные продукты и услуги становятся все более важными, оттесняя материальные блага на второй план.

Процессы информатизации связаны с использованием разнообразных информационно-коммуникационных технологий и систем. Потребность в разработке и применении эффективных информационных решений постоянно возрастает.

Информационная война направлена на нанесение ущерба ключевым структурам другой стороны, а также на дестабилизацию ее социальной и политической системы. Она представляет собой форму межгосударственного соперничества, осуществляемого через информационное воздействие на управленческие системы и общество другого государства [4].

Информационная преступность заключается в незаконных действиях с использованием информационного пространства с целью достижения противоправных целей.

Информационное воздействие также включает в себя распространение дезинформации, провокации и создание манипулятивных сообщений с целью дестабилизации ситуации, формирования определенного общественного мнения или воздействия на поведение целевой аудитории. Оно может быть использовано как для достижения политических или военных целей, так и для экономического

*Таблица 1*

**Сравнительная характеристика традиционной и цифровой экономики**

| Показатели | Информационная безопасность | Традиционная экономика | Цифровая экономика |
|---|---|---|---|
| Рост угроз в сети | Требует постоянного обновления мер безопасности | Редкие случаи хакерских атак | Частые атаки хакеров и вирусов |
| Киберпреступность | Множество методов атак на информацию | Ограниченные угрозы | Высокая вероятность киберпреступности |
| Данные и конфиденциальность | Необходимо защищать конфиденциальные данные от несанкционированного доступа | Меньшая зависимость от цифровых данных | Огромное количество цифровых данных, требующих защиты |
| Бюджет на информационную безопасность | Требует значительных инвестиций | Траты на безопасность меньше, чем на другие сферы | Увеличение бюджета на информационную безопасность |
| Доверие потребителей к защите данных | Критически важно для поддержания доверия потребителей | Меньшая вероятность утечки данных | Несоблюдение правил безопасности может привести к потере доверия потребителей |
| Взаимодействие между компаниями | Обмен информацией требует дополнительных мер защиты | Меньше рисков при обмене информацией | Необходимость усиленной защиты при обмене данными в цифровой экономике |

или социального воздействия, распространения дезинформации или полезной информации в обществе, воздействия на мнение и психику различных социальных групп.

Из приведенного выше можно сделать вывод, что информационная безопасность означает защиту объектов безопасности и их свойств от вредоносного воздействия информации и информационной инфраструктуры [5].

К основным угрозам информационной безопасности относятся:

1. Вредоносное программное обеспечение.

Киберпреступники используют вредоносное программное обеспечение для заражения компьютеров и кражи конфиденциальной информации.

2. Фишинг.

Киберпреступники обманывают пользователей, чтобы получить доступ к их учетным данным, паролям и другой конфиденциальной информации.

3. Хакерские атаки.

Хакеры используют DDoS-атаки, сетевые сканеры и эксплойты уязвимостей для проникновения в корпоративные сети и кражи информации.

4. Неправомерный доступ.

Неправомерный доступ к конфиденциальной информации может привести к ее утечке и использованию во вредных целях.

5. Недостаточная защита данных.

Слабые пароли, неправильные настройки безопасности и отсутствие резервного копирования данных могут привести к утечке конфиденциальной информации.

6. Манипуляции с данными и фейковые новости.

Манипуляции с данными и фейковые новости могут привести к введению пользователей в заблуждение и распространению дезинформации.

Для обеспечения безопасности цифровизации и информатизации экономических процессов необходимо усилить меры защиты [6].

## Результаты

На российском рынке деятельности по созданию и внедрению современных информационных технологий успешно функционируют несколько сервис-провайдеров и фирм. Однако, чтобы поддерживать этот уровень развития, необходимо усовершенствовать технологии защиты (табл. 2).

*Таблица 2*

**Важные аспекты информационной безопасности в экономике**

| Аспект | Традиционная экономика | Цифровая экономика |
|---|---|---|
| Объем информации | Ограниченный | Большой |
| Скорость передачи | Медленная | Быстрая |
| Способ обработки | Ручная | Автоматизированная |
| Уязвимость к угрозам | Низкая | Высокая |
| Риск утечки данных на защиту | Низкий | Высокий |
| Затраты на защиту | Небольшие | Значительные |
| Важность для экономики | Не столь критична | Очень важная |

К числу инструментов обеспечения информационной безопасности цифровой экономики можно отнести следующее:

1. Многофакторная аутентификация, такая как использование паролей и биометрических данных.

2. Шифрование данных для защиты информации от несанкционированного доступа.

3. Мониторинг и анализ событий для раннего обнаружения угроз безопасности.

4. Регулярное обновление программного обеспечения с целью закрытия уязвимостей и обновления защиты.

5. Обучение сотрудников информационной безопасности для профилактики социальной инженерии и других атак.

Примером успешного обеспечения информационной безопасности в экономике являются:

1. Стандартизация и сертификация информационных систем и технологий – разработка и внедрение стандартов для систем управления информационной безопасностью, а также получение сертификатов на соответствие данным стандартам.

2. Внедрение систем защиты информации, в частности, систем шифрования, аутентификации и авторизации, систем контроля доступа к информационным ресурсам, а также систем обнаружения и предотвращения вторжений.

3. Обучение и повышение квалификации сотрудников путем регулярного проведения тренингов и семинаров по вопросам информационной безопасности, а также организации курсов повышения квалификации и сертификации специалистов.

4. Разработка и внедрение политики информационной безопасности. Успешная деятельность в данном направлении предполагает определение целей и задач, разработку процедур и регламентов, обучение персонала, анализ результатов.

5. Применение современных технологий и решений в области информационной безопасности – использование виртуальных частных сетей (VPN), технологии блокчейн для обеспечения безопасности финансовых транзакций, искусственного интеллекта для мониторинга и анализа информационных систем.

6. Тесное сотрудничество с правоохранительными органами и регуляторами – регулярное участие в мероприятиях, организованных государственными органами, обмен информацией и опытом, проведение совместных расследований и обучающих программ.

7. Тесное сотрудничество с поставщиками и партнерами. Успешное управление информационной безопасностью предполагает тесное сотрудничество с поставщиками услуг и партнерами, чтобы гарантировать, что они придерживаются тех же стандартов и принципов информационной безопасности, что и организация.

8. Обеспечение непрерывности бизнеса и восстановления после инцидентов. Пример успешного обеспечения информационной безопасности включает наличие планов действий на случай чрезвычайных ситуаций и инцидентов, связанных с нарушением информационной безопасности, и обеспечение возможности быстрого восстановления работы организации после таких инцидентов.

9. Аутентификация и авторизация пользователей – внедрение надежных механизмов аутентификации и авторизации пользователей для предотвращения несанкционированного доступа к информационным системам и ресурсам.

10. Регулярный мониторинг и тестирование систем. Успешное обеспечение информа-

ционной безопасности также включает проведение регулярного мониторинга и тестирования систем для обнаружения уязвимостей и слабых мест, а также внедрение процессов для их устранения.

11. Внедрение системы менеджмента информационной безопасности (ISMS). Успешные организации внедряют и сертифицируют систему менеджмента информационной безопасности согласно стандартам, таким как ISO 27001, для управления рисками и обеспечения соответствия требованиям безопасности.

## Обсуждение

Электронные цифровые подписи также эффективно применяются в различных сферах, включая государственные закупки и электронные торги.

Компании могут помочь своим сотрудникам обеспечить информационную безопасность, следуя простым правилам «цифровой гигиены», таким как:

1. Не переходить по ссылкам, отправленным незнакомыми людьми на почту или мессенджер, так как в данных ссылках могут быть зашифрованы вредоносные программы, которые могут распространяться через почту и социальные сети.

2. Обновлять программное обеспечение и использовать антивирусы. Антивирусное ПО является необходимым условием для защиты от вредоносных программ и нежелательных вирусов. Обновление программного обеспечения также способствует своевременному выявлению и предотвращению сторонних угроз.

3. Не открывать вложения и сообщения от посторонних лиц, а также никогда не отправлять свои персональные данные через социальные сети и электронную почту. При отправке сообщения возможен его перехват злоумышленником для извлечения и дальнейшего использования конфиденциальной информации.

4. Не использовать в персональных компьютерах посторонние носители информации. Внешние носители информации могут быть заражены вредоносным кодом. Данные устройства могут привести к утечкам персональной информации путем имитации программы и моделирования поведения таким образом, чтобы внутренние системы устройства приняли его за подобное.

5. Пользоваться только проверенными сайтами. При переходе на непроверенные сайты существует риск стать объектом мошенников. Пройдя на сайт, содержащий вредоносные программы, может автоматически запуститься скачивание вирусов.

6. Использовать сложные пароли. Сложные пароли являются ключевым фактором защиты персонального компьютера. Длинные пароли, специальные символы, смешение символом, нижних и верхних регистров повышают защищенность учетной записи. Использование одного пароля на нескольких учетных записях не является безопасным.

7. Резервное копирование данных. Данный метод позволяет защитить документы и важные файлы от заражения устройства вредоносными программами и вирусами.

8. Использовать для работы и личного пользования отдельные персональные устройства. При использовании одного устройства для работы и развлекательного серфа в интернете возможна угроза безопасности данных.

Для развития культуры информационной безопасности необходимо проводить регулярные тренинги и семинары в целях повышения осведомленности сотрудников, а также обеспечить открытость корпоративных служб информационной безопасности для взаимодействия с коллегами из других подразделений.

В программе «Цифровая экономика» информационная безопасность в России отмечена как важный раздел, который обсуждается в экспертных группах. Состояние информационной безопасности в стране считается зрелым и успешным, охватывая множество отраслей, связанных с информационными технологиями [7].

Информационная безопасность влияет на множество отраслей, которые зависят от информационных технологий. Решая проблемы своей отрасли, эксперты также вносят вклад в экономику в целом. Однако сегодня технологии нельзя рассматривать отдельно от кадровых вопросов: специалисты не только создают и обслуживают технологии, но и обеспечивают их безопасность. Поэтому подготовка высоко-

квалифицированных специалистов в области инфраструктуры информационных технологий имеет такое же важное значение, как и обеспечение информационной безопасности [8].

## Заключение

Таким образом, необходимо отметить, что цифровая экономика не может существовать без информационной безопасности, что делает ее важной не только для специалистов по безопасности, но и для всех участников процесса разработки, тестирования и использования информационных технологий. В наше время это актуальная тема для развития страны. Защита данных государства, общества и личности становится приоритетной задачей цифровой экономики в условиях повсеместной автоматизации и цифровизации.

Развитие цифровой экономики открывает новые возможности для создания «умных» городов, транспорта и сельского хозяйства. Кроме того, повышается уровень цифровой грамотности населения и уменьшается цифровое неравенство между регионами. Тем не менее следует учитывать и такие риски, как нарушение конфиденциальности данных, засорение информационного пространства, дефицит квалифицированных кадров и возможное увеличение безработицы из-за автоматизации процессов в цифровой экономике [9].

Для обеспечения устойчивого развития цифровой экономики необходимо уделить внимание информационной безопасности, повысить уровень культуры и проводить обучение по защите информации, разработать эффективную политику в этой области и постоянно обновлять нормативно-правовую базу. Распространение цифровой экономики во многом зависит от обеспечения информационной безопасности и защиты информационных систем от новых рисков и уязвимостей, что является ключевым аспектом для дальнейшего прогрессивного развития национальной экономики и повышения ее конкурентоспособности на мировом рынке. Поэтому необходимо продолжать развивать цифровую экономику, внедряя ее во всех сферах деятельности и обеспечивая безопасность информации [7].

## Список источников

1. Асаул В.В., Михайлова А.О. Обеспечение информационной безопасности в условиях формирования цифровой экономики // Теория и практика сервиса: экономика, социальная сфера, технологии. 2018. № 4 (38). С. 5–9.

2. Цифровая экономика : [сайт]. URL: https://d-economy.ru/ (дата обращения: 18.01.2024).

3. Маркова В.Д. Цифровая экономика : учеб. Москва : ИНФРА-М, 2018. 186 с.

4. Минзов А.С., Невский А.Ю., Баронов О.Ю. Информационная безопасность в цифровой экономике // ИТНОУ: информационные технологии в науке, образовании и управлении. 2018. № 3 (7). С. 52–59.

5. Цифровая грамотность для экономики будущего / Л.Р. Баймуратова, О.А. Долгова, Г.Р. Имраева [и др.] ; Аналитический центр НАФИ. Москва : Изд-во НАФИ, 2018. 86 с.

6. Информационная безопасность сквозь призму цифровой экономики / Ф.А. Хочуева, Т.Л. Шугунов, А.З. Жуков, Ч.Х. Ингушев // Современные наукоемкие технологии. 2018. № 11-1. С. 65–71.

7. Зарафетдинова Э.Р., Матягина Т.В. Информационная безопасность цифровой экономики России // E-Scio. 2022. № 10 (73). С. 353–358.

8. Назарова Д., Башимова Н. Важность информационной безопасности в цифровой экономике // Символ науки. 2023. № 5-1. С. 84–85.

9. Акмяммедов М.Р. Защита данных и информационная безопасность в условиях цифровой экономики // Всемирный ученый. 2024. № 19. URL: https://cyberleninka.ru/article/n/zaschita-dannyh-i-informatsionnaya-bezopasnost-v-usloviyah-tsifrovoy-ekonomiki (дата обращения: 18.01.2024).

## References

1. Asaul V.V., Mikhailova A.O. Ensuring information security in the conditions of the formation of the digital economy // Theory and practice of the service: economics, social sphere, technology. 2018. No. 4 (38). Pp. 5–9.

2. Digital economy : [website]. URL: https://d-economy.ru/ (date of access: 18.01.2024).

3. Markova V.D. Digital economy : textbook. Moscow : INFRA-M, 2018. 186 p.

4. Minzov A.S., Nevsky A.Yu., Baronov O.Yu. Information security in the digital economy // ITNOU: Information technologies in science, education and management. 2018. No. 3 (7). Pp. 52–59.

5. Digital literacy for the economy of the future / L.R. Baymuratova, O.A. Dolgova, G.R. Imraeva [et al.] ; NAFI Analytical Center. Moscow : NAFI Publishing House, 2018. 86 p.

6. Information security through the prism of the digital economy / F.A. Khochueva, T.L. Shugunov, A.Z. Zhukov, Ch.H. Ingushev // Modern high-tech technologies. 2018. No. 11-1. Pp. 65–71.

7. Zarafetdinova E.R., Matyagina T.V. Information security of the digital economy of Russia // E-Scio. 2022. No. 10 (73). Pp. 353–358.

8. Nazarova D., Bashimova N. The importance of information security in the digital economy // Symbol of Science. 2023. No. 5-1. Pp. 84–85.

9. Akmyammedov M.R. Data protection and information security in the digital economy // World Scientist. 2024. No. 19. URL: https://cyberleninka.ru/article/n/zaschita-dannyh-i-informatsionnaya-bezopasnost-v-usloviyah-tsifrovoy-ekonomiki (date of access: 18.01.2024).

*Информация об авторах*

*К.О. Карлышева* – студент Поволжского государственного университета телекоммуникаций и информатики;
*А.Р. Булатова* – студент Поволжского государственного университета телекоммуникаций и информатики;
*М.И. Иваев* – старший преподаватель кафедры «Цифровая экономика» Поволжского государственного университета телекоммуникаций и информатики.

*Information about the authors*

*K.O. Karlysheva* – student of the Volga Region State University of Telecommunications and Informatics;
*A.R. Bulatova* – student of the Volga Region State University of Telecommunications and Informatics;
*M.I. Ivaev* – senior lecturer of the Department of Digital Economics of the Volga Region State University of Telecommunications and Informatics.

Статья поступила в редакцию 19.03.2024; одобрена после рецензирования 07.05.2024; принята к публикации 27.05.2024.
The article was submitted 19.03.2024; approved after reviewing 07.05.2024; accepted for publication 27.05.2024.