

ЗАЩИТА ИНФОРМАЦИИ И ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ В ЭПОХУ ЦИФРОВЫХ ТЕХНОЛОГИЙ

К. А. Смолякова

*студент, Белорусский государственный университет пищевых и химических технологий, г. Могилев,
Беларусь, smoliakovakarina@gmail.com*

Научный руководитель **Н. А. Шалабодова**

*старший преподаватель, Белорусский государственный университет пищевых и химических
технологий, г. Могилев, Беларусь, nshalabodova@mail.ru*

В условиях стремительной цифровизации экономики вопросы об экономической безопасности и защиты информации приобретают особую актуальность. В статье рассмотрены ключевые угрозы, возникающие в цифровой среде, а также методы обеспечения устойчивости экономики и сохранности данных. Отдельное внимание уделено международным стандартам, нормативной базе и балансу между инновациями и рисками.

Ключевые слова: цифровизация; экономическая безопасность; защита информации.

INFORMATION PROTECTION AND ECONOMIC SECURITY IN THE DIGITAL AGE

K. A. Smolyakova

*student, Belarusian State University of Food and Chemical Technologies, Mogilev, Belarus,
smoliakovakarina@gmail.com*

Supervisor **N. A. Shalabodova**

*senior lecturer, Belarusian State University of Food and Chemical Technologies, Mogilev, Belarus,
nshalabodova@mail.ru*

In the context of rapid digitalization of the economy, issues related to economic security and information protection are becoming increasingly important. This article explores the key threats that arise in the digital environment, as well as the methods for ensuring economic resilience and data protection. Special attention is given to international standards, regulatory frameworks, and the balance between innovation and risk.

Keywords: digitalization; economic security; information protection.

Цифровизация охватывает все сферы современной жизни – от финансов и торговли до государственного управления и личной коммуникации. С одной стороны, она открывает новые возможности для роста и эффективности, с другой – порождает новые угрозы, особенно в области экономической безопасности и защиты информации. Устойчивость экономики напрямую зависит от способности противостоять киберугрозам, утечкам данных и технологическим сбоям.

Экономическая безопасность – это обеспечение защищенности национальной и корпоративной экономики от внутренних и внешних угроз, позволяющие стабильно функционировать и развиваться.

Цифровая эпоха привнесла новые риски в дополнение к традиционным:

- 1) кибератаки на финансовые и государственные учреждения;
- 2) цифровой шпионаж и промышленный саботаж;
- 3) зависимость от иностранных цифровых платформ и облачных сервисов;
- 4) уязвимость критической инфраструктуры (энергетика, транспорт, связь).

Примером может служить инцидент с компанией Equifax в 2017 году, когда в результате кибератаки были похищены персональные данные более 147 миллионов клиентов [5]. Это привело к падению акций, потере доверия и многомиллионным убыткам.

Информационная безопасность – это состояние защищённости информационной среды от утечки, несанкционированного и непреднамеренного воздействия на защищаемую информацию. Защита информации, в свою очередь, представляет собой совокупность мероприятий и процессов, направленных на достижение данного состояния [3]. В цифровую эпоху она становится неотъемлемой частью экономической безопасности. Основные направления:

- 1) внедрение международных стандартов, таких как ISO/IEC 27001 [6];
- 2) управление рисками и инцидентами;
- 3) обучение персонала и контроль доступа;
- 4) создание резервных копий.

Нормативная база в Республике Беларусь также адаптируется к цифровым реалиям, включая положения о защите персональных данных и кибербезопасности [4].

Цифровизация позволяет оптимизировать процессы, снижать издержки и повышать прозрачность. Однако без должной защиты инновации могут обернуться катастрофой. Поэтому важно развивать отечественные технологии и платформы, внедрять гибкие модели управления рисками, поддерживать цифровую грамотность населения и бизнеса, развивать международное сотрудничество в сфере кибербезопасности.

Примером сбалансированного подхода может служить использование технологий блокчейн: они одновременно обеспечивают прозрачность и требуют новых методов защиты [6].

Современные угрозы носят транснациональный характер, поэтому вопросы экономической и информационной безопасности невозможно решать исключительно на национальном уровне. Кибератаки часто исходят из-за рубежа, а цифровые платформы и облачные сервисы принадлежат международным корпорациям. В этой связи особое значение приобретает участие Беларуси и других стран в международных организациях, таких как ООН, ОБСЕ и ШОС, где формируются общие подходы к кибербезопасности и защите критической инфраструктуры [7].

Для повышения уровня защиты активно применяются современные технологии: системы искусственного интеллекта для выявления аномалий, биометрическая аутентификация, квантовое шифрование. Эти инструменты позволяют не только предотвращать атаки, но и прогнозировать потенциальные угрозы. Однако внедрение таких решений требует значительных инвестиций и подготовки специалистов, что делает актуальным вопрос государственной поддержки и стимулирования инноваций в сфере кибербезопасности [1].

Кибератаки и утечки данных оказывают прямое влияние на экономику: снижают доверие инвесторов, приводят к падению рыночной стоимости компаний, увеличивают расходы на восстановление систем. По оценкам международных экспертов, глобальный ущерб от киберпреступности в 2024 году превысил 8 триллионов долларов [2]. Для Беларуси и других стран с развивающейся цифровой экономикой это означает необходимость учитывать киберриски в стратегическом планировании и национальной политике безопасности.

Экономическая безопасность и защита информации в эпоху цифровизации – это про стратегические приоритеты. Устойчивость государства, бизнеса и общества зависит от способности адаптироваться к новым угрозам, развивать цифровую инфраструктуру и обеспечивать надёжную защиту данных. Только комплексный подход позволит сохранить стабильность и реализовать потенциал цифровой экономики.

Библиографические ссылки

1. *Clarke R., Knake R.* Cyber War: The Next Threat to National Security. New York : HarperCollins, 2020.
2. Cybersecurity Ventures. 2024 Cybercrime Report. URL: <https://cybersecurityventures.com/cyber-crime-report/> (дата обращения: 14.09.2025).
3. *Гончаров А. В.* Информационная безопасность: теория и практика. М. : Юрайт, 2021.
4. Закон Республики Беларусь «Об информации, информатизации и защите информации». URL: <https://pravo.by/document/?guid=3871&p0=h10800455> (дата обращения 14.09.2025).
5. *Кузнецов Н. В.* Цифровая экономика и киберугрозы. СПб. : Питер, 2022. 192 с.
6. Стандарт ISO/IEC 27001:2022 – Международный стандарт по управлению информационной безопасностью. URL: <https://pqm-online.com/assets/files/pubs/translations/std/iso-mek-27001-2022.pdf> (дата обращения 14.09.2025).
7. International Telecommunication Union. Global Cybersecurity Index 2021. Женева : ITU, 2021.