КИБЕРБЕЗОПАСНОСТЬ КАК НЕОТЪЕМЛЕМАЯ ЧАСТЬ УСТОЙЧИВОЙ ЦИФРОВОЙ ЭКОНОМИКИ

Бабаева Сабинабону Давронбек қизи
ТДТУ кафедра экономики транспорта, группа РИК-3, студент 2 курса
Тел: +998505002540
Электронная почта: babaevas044@gmail.com

Аннотация. *Статья раскрывает ключевую роль кибербезопасности в обеспечении устойчивости цифровой экономики. На фоне ускоренной цифровизации возрастают как экономическая зависимость от цифровых платформ, так и уязвимость к киберугрозам. Рассматриваются основные векторы угроз, экономические последствия киберинцидентов и актуальные меры защиты на национальном и международном уровнях. Представлен анализ тенденций роста потерь от кибератак. Обоснована необходимость системного подхода к формированию киберустойчивости как части макроэкономической стратегии.*

Ключевые слова: *кибербезопасность, цифровая экономика, устойчивое развитие, киберугрозы, цифровая трансформация, защита данных*.

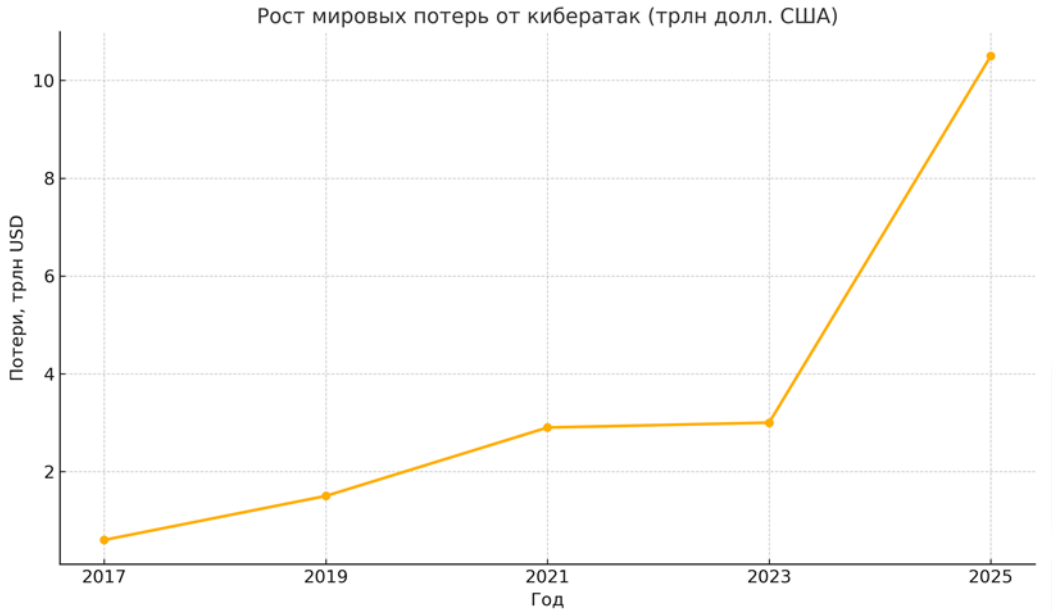
Annotation. *The article highlights the critical role of cybersecurity in ensuring the sustainability of the digital economy. Amid accelerated digitalization, both economic dependence on digital platforms and vulnerability to cyber threats are increasing. The paper examines the main vectors of cyber threats, the economic consequences of cyber incidents, and current protective measures at the national and international levels. It provides an analysis of the growing financial losses caused by cyberattacks and substantiates the need for a systematic approach to building cyber resilience as part of a broader macroeconomic strategy.*

Key words: *cybersecurity, digital economy, sustainable development, cyber threats, digital transformation, data protection.*

Цифровая экономика стремительно трансформирует глобальные и национальные рынки. В основе этих изменений лежат технологии интернета вещей, облачные вычисления, искусственный интеллект, большие данные и блокчейн. Однако активная цифровизация неразрывно связана с ростом киберугроз. В этих условиях устойчивость экономики в цифровую эпоху становится невозможной без эффективной и гибкой системы кибербезопасности, способной отвечать на новые вызовы. Одним из наиболее уязвимых звеньев современной цифровой инфраструктуры являются цифровые платформы, которые уже стали критически важными компонентами национальной экономики. Любая их уязвимость — от утечек конфиденциальных данных до дестабилизации логистических и энергетических систем — может обернуться серьёзными макроэкономическими последствиями. Так, в 2021 году атака на Colonial Pipeline вызвала перебои в поставках топлива в США, а в 2022 году масштабная утечка данных в компании T-Mobile

затронула более 37 миллионов пользователей, повлекшая за собой как репутационные, так и финансовые потери. Растущая зависимость экономики от цифровых систем требует количественной оценки возникающих рисков. По данным Cybersecurity Ventures, мировой экономический ущерб от кибератак в 2023 году составил около $3 трлн, а к 2025 году может достигнуть $10,5 трлн. Такие показатели сопоставимы с ВВП крупнейших экономик мира, что подчёркивает масштаб угрозы. Важно отметить, что с 2017 года потери от киберинцидентов увеличились более чем в пять раз. Это свидетельствует не только об эволюции и усложнении методов атак, но и о недостаточной готовности государств и компаний к изменениям в цифровом ландшафте.

Для наглядной иллюстрации тенденций представлен следующий график:



Как видно из графика, потери от киберугроз демонстрируют устойчивую экспоненциальную динамику, что требует системных мер реагирования как на национальном, так и на международном уровне. Для ответа на эти вызовы государства активно разрабатывают стратегические документы в области кибербезопасности. В Европейском союзе реализуется «Цифровой компас 2030», особое внимание в котором уделяется формированию центров киберустойчивости и обновлению законодательства в рамках директивы NIS2. В США утверждена Национальная стратегия кибербезопасности 2023 года, направленная на повышение ответственности разработчиков программного обеспечения и инвестиции в человеческий капитал. В Узбекистане также наблюдается прогресс: реализуется Концепция кибербезопасности до 2026 года, развиваются SOC-центры и внедряются цифровые удостоверения личности. Таким образом, кибербезопасность всё более интегрируется в концепцию

устойчивого развития. Надёжная защита цифровых прав граждан, бесперебойность работы цифровых сервисов, а также минимизация экономических потерь от инцидентов становятся ключевыми элементами как внутренней политики государств, так и международного взаимодействия. В условиях глобальной конкуренции доверие к цифровой инфраструктуре напрямую влияет на привлекательность страны для инвесторов и партнёров. Центральным элементом современной цифровой среды является цифровая идентичность. В связи с ростом количества онлайн-сервисов и цифровизацией государственных функций особое значение приобретает надёжная защита персональных данных. В ЕС для этих целей был принят Общий регламент по защите данных (GDPR), который стал моделью для многих стран. Узбекистан также предпринимает шаги в этом направлении — разрабатываются соответствующие стандарты, формируется реестр пользователей электронных услуг. Однако, несмотря на усилия, сохраняются риски, связанные с фишингом, утечками данных и цифровым мошенничеством. Эффективное противодействие этим угрозам невозможно без развитого кадрового потенциала. В настоящее время мировой рынок испытывает острый дефицит квалифицированных специалистов в области информационной безопасности — по оценкам (ISC)², нехватка превышает 3 миллиона человек. В этой связи возрастающую роль играют государственные программы подготовки и переподготовки кадров, университетские курсы и внедрение основ цифровой гигиены в систему общего образования. Дополнительно важно международное сотрудничество: крупные ИТ-компании (например, Microsoft, Cisco, IBM) реализуют глобальные программы по обучению и сертификации специалистов в этой сфере. Отдельного внимания требует финтех-сектор, находящийся на передовой цифровой трансформации. Его уязвимость обусловлена тем, что финансовые сервисы обрабатывают чувствительные данные и совершают критически важные операции. Злоумышленники всё чаще применяют фишинг, перехват сообщений, взлом приложений. Это не только создаёт угрозу для отдельных пользователей, но и формирует системные риски. Как следствие, недоверие к цифровым финансовым сервисам снижает темпы цифровизации банковской системы. Для преодоления этих барьеров компании внедряют биометрическую аутентификацию, системы искусственного интеллекта для мониторинга подозрительных операций и усиливают защиту мобильных платформ. Одним из наиболее эффективных подходов к повышению киберустойчивости является государственно-частное партнёрство. В условиях быстро меняющегося ландшафта угроз кооперация между государственными структурами и бизнесом

становится необходимостью. Государства обеспечивают нормативно-правовую основу, тогда как частный сектор — оперативную технологическую реализацию. Примеры включают совместные киберучения, обмен информацией об угрозах (через ISAC), разработку и внедрение стандартов защиты. Тем не менее правовая база в области кибербезопасности во многих странах всё ещё догоняет технологический прогресс. Возникают новые вызовы: вопросы юрисдикции, трансграничного обмена данными, цифрового суверенитета. Это требует обновления международных соглашений и выработки универсального подхода. В Узбекистане ведётся работа по адаптации международных норм, включая положения Будапештской конвенции. В перспективе возможна разработка глобального кодекса поведения в киберпространстве, аналогичного Парижскому соглашению по климату.

В заключение стоит отметить тот факт, что кибербезопасность и цифровая экономика не просто пересекаются — они образуют единое целое. Устойчивость цифровой экономики невозможна без системной и превентивной киберполитики. Только при условии масштабных инвестиций в технологии, кадры, институты и международную кооперацию возможно обеспечить цифровое будущее, устойчивое к внутренним и внешним угрозам.

Список использованной литературы:

1. Касперский Е.В. Киберугрозы и цифровая безопасность: вызовы XXI века // Информационное общество. — 2021. — №4. — С. 17–25.
2. Куликов А.С., Миронов И.А. Стратегии кибербезопасности в условиях цифровой трансформации экономики // Вестник Российской экономической школы. — 2022. — Т. 26, №3. — С. 112–124.
3. Cybersecurity Ventures. 2023 Official Annual Cybercrime Report. — [Электронный ресурс]. — Режим доступа: https://cybersecurityventures.com (дата обращения: 11.07.2025).
4. McKinsey & Company. Global cybersecurity outlook 2023. — [Электронный ресурс]. — Режим доступа: https://www.mckinsey.com/business-functions/risk (дата обращения: 11.07.2025).
5. Akhmadzhonova, G., Nazhmutdinova, D., Negmatshoeva, K., & Iroda, K. (2024). Assessment of the Microbial Flora of the Genital Tract and the Morphofunctional State of the Endometrium in Antiphospholipid Syndrome.
6. Regulation (EU) 2016/679 of the European Parliament and of the Council (GDPR). — Official Journal of the European Union. — 2016.
7. Nabijonova, G. M., & Kamilova, I. A. (2025). Robson classification for caesarean section (Doctoral dissertation, O'zbekiston).
8. Рахматов, Ф. О., & Нуриев, К. К. (2022). Исследование плодов дыни как объекта технической переработки. Илмий мақолалар тўплами, 330.