# ЦЕНА ЦИФРОВОЙ БЕЗОПАСНОСТИ: КАК КИБЕРУГРОЗЫ ФОРМИРУЮТ НОВУЮ ЭКОНОМИКУ

Нурматов Муроджон Дильшод угли[1], Таджиходжаева Эльвира Рашидовна[2]

[1] Студент направления «Кибербезопасность» Ташкентского международного университета "Tashkent International University of Education"
[2] Ташкентский международный университет "Tashkent International University of Education"
[1] E-mail: U25068@tiue.uz
[2] E-mail: t414@tiue.uz
DOI: 10.61587/mmit.tiue.uz.v1i1.415

**Аннотация.** В статье кибербезопасность рассматривается как значимый фактор трансформации современной мировой экономики и формирования новой отрасли, ориентированной на защиту цифровых ресурсов. Проанализированы актуальные тенденции роста киберугроз, их влияние на деятельность коммерческих организаций и государственных структур, а также экономические и репутационные последствия крупных инцидентов информационной безопасности. Особое внимание уделяется мерам реагирования на киберугрозы, включая развитие технологических решений, расширение кадрового потенциала в сфере информационной безопасности и формирование национальных стратегий киберзащиты. Отдельно обозначены перспективы развития данной отрасли в условиях распространения искусственного интеллекта, облачных технологий и интернета вещей, а также роль цифровой грамотности как важнейшего компонента современной системы обеспечения безопасности.

***Ключевые слова:*** *кибербезопасность, киберугрозы, кибератаки, цифровая экономика, информационная безопасность, цифровая грамотность, искусственный интеллект, облачные технологии, интернет вещей, защита данных, национальная киберзащита.*

# THE COST OF DIGITAL SECURITY: HOW CYBER THREATS SHAPE A NEW ECONOMY

Nurmatov Murodjon Dilmurod ugli[1], Elvira Rashidovna Tadjikhodjaeva[2]

[1] Student of the "Cybersecurity" Program "Tashkent International University of Education"
[2] "Tashkent International University of Education"
[1] E-mail: U25068@tiue.uz
[2] E-mail: t414@tiue.uz

**Abstract.** The article examines cybersecurity as a significant factor in the transformation of the modern global economy and the formation of a new industry focused on protecting digital resources. Current trends in the growth of cyber threats, their impact on commercial organizations and government institutions, as well as the economic and reputational consequences of major information security incidents are analyzed. Particular attention is paid to measures for responding to cyber threats, including the development of technological solutions, the expansion of human resources potential in the field of information security, and the formation of national cybersecurity strategies. The article also highlights the prospects for the development of this field in the context of the widespread adoption of artificial intelligence, cloud technologies, and the Internet of Things, as well as the role of digital literacy as an essential component of the modern security system.

***Keywords:*** *cybersecurity, cyber threats, cyberattacks, digital economy, information security, digital literacy, artificial intelligence, cloud technologies, Internet of Things, data protection, national cybersecurity.*

## Введение

Цифровая трансформация современного общества сопровождается ростом роли информационных ресурсов и, как следствие, повышением значимости их защиты, поскольку государственные структуры, бизнес и повседневная жизнь всё теснее связаны

с электронными сервисами, базами данных и сетевыми коммуникациями; в связи с этим кибербезопасность становится одним из ключевых направлений обеспечения устойчивого развития и цифрового суверенитета, что отражено в «Стратегии кибербезопасности Узбекистана на 2026–2030 годы» [1].

В современном мире цифровые технологии стали неотъемлемой частью жизни общества. Практически каждый человек ежедневно использует интернет, облачные сервисы, социальные сети, электронную почту и онлайн-банкинг. Цифровизация затронула не только обычных пользователей, но и крупнейшие компании, государственные организации, банки и даже системы здравоохранения [3, 14]. Сегодня информация стала одним из самых ценных ресурсов современности, а её защита — одной из важнейших задач [8].

Компании всё чаще переходят на электронные базы данных, облачные хранилища и автоматизированные системы управления. Это значительно упрощает работу, ускоряет обмен информацией и повышает производительность труда. Однако вместе с развитием технологий появляются новые угрозы. Хакеры и киберпреступники постоянно ищут способы получить доступ к конфиденциальной информации, банковским счетам и внутренним системам компаний.

В последние годы проблема кибербезопасности стала особенно актуальной. Если раньше кибератаки воспринимались как редкие случаи, то сегодня они происходят ежедневно [11]. Многие компании сталкиваются с утечками данных, вирусными атаками и попытками взлома. При этом далеко не все организации готовы вкладывать достаточные средства в защиту своих систем. Часто компании уделяют больше внимания развитию продукта и увеличению прибыли, забывая о цифровой безопасности. Однако любая утечка данных может привести не только к финансовым потерям, но и к разрушению репутации компании [5].

Известный американский предприниматель и основатель Microsoft Билл Гейтс однажды сказал: «Информация — это новая нефть XXI века». Эта фраза особенно актуальна в современном цифровом обществе, где данные пользователей стали огромной ценностью как для бизнеса, так и для злоумышленников [10].

Вопросы обеспечения кибербезопасности становятся приоритетным направлением государственной политики многих стран мира, включая Узбекистан. В последние годы в Республике Узбекистан активно разрабатываются стратегии цифрового развития и национальной киберзащиты, направленные на укрепление информационной безопасности и защиту цифровой инфраструктуры страны [2].

**Развитие киберугроз в современном мире**

С каждым годом количество кибератак в мире стремительно увеличивается. Развитие цифровых технологий открыло перед человечеством множество возможностей, однако одновременно создало и новые риски [11, 13]. Хакеры используют современные методы взлома, вредоносное программное обеспечение, вирусы-вымогатели и фишинговые атаки для получения доступа к конфиденциальной информации.

Одной из главных целей злоумышленников являются персональные данные пользователей. Это могут быть банковские карты, пароли, электронные адреса, фотографии, документы и даже медицинская информация. Полученные данные нередко используются для мошенничества, шантажа или продажи на теневых интернет-площадках.

Особенно уязвимыми становятся крупные компании и международные корпорации, поскольку они хранят огромные объёмы информации о своих клиентах. Одним из наиболее известных примеров стала масштабная утечка данных компании

Yahoo, в результате которой были скомпрометированы данные миллионов пользователей. Данный инцидент стал одним из крупнейших случаев нарушения информационной безопасности в истории интернета и серьёзно повлиял на репутацию компании [10].

Другим показательным примером является компания Equifax — одно из крупнейших кредитных агентств США. В 2017 году злоумышленники получили доступ к персональным данным более 140 миллионов человек, включая номера социального страхования и банковскую информацию. Последствия этой кибератаки привели к крупным финансовым потерям и необходимости выплаты многомиллионных компенсаций пострадавшим пользователям [12].

**Экономические последствия кибератак**

Кибератаки оказывают значительное влияние на мировую экономику. Финансовые потери компаний после взломов могут достигать миллиардов долларов. Убытки возникают не только из-за кражи денежных средств, но и вследствие остановки работы цифровых систем, потери клиентов и необходимости восстановления инфраструктуры [6].

После крупных утечек данных организации вынуждены восстанавливать повреждённые системы, усиливать механизмы защиты, выплачивать компенсации клиентам, оплачивать штрафы и привлекать дополнительных специалистов по информационной безопасности. Всё это требует серьёзных финансовых затрат. Кроме материального ущерба, компании сталкиваются с падением доверия со стороны пользователей. В условиях цифровой экономики репутация становится одним из важнейших активов организации. Если компания допускает утечку конфиденциальной информации, клиенты начинают сомневаться в её надёжности и безопасности предоставляемых услуг [5].

Известный специалист по кибербезопасности Брюс Шнайер отмечал: «Безопасность — это не продукт, а процесс». Данная мысль подчёркивает, что защита информации требует постоянного развития, обновления технологий и регулярных инвестиций. Недостаточно один раз установить антивирусную программу или систему защиты — безопасность должна совершенствоваться непрерывно в соответствии с развитием новых угроз и методов кибератак [13].

**Формирование новой экономики кибербезопасности.**

Рост числа киберугроз обусловил формирование новой и весьма динамичной отрасли современной экономики — индустрии кибербезопасности. В условиях цифровизации бизнес-процессов, развития электронных сервисов и увеличения объёмов обрабатываемых данных организации по всему миру вынуждены направлять значительные ресурсы на защиту информации, цифровой инфраструктуры и пользовательских данных [14]. Таким образом, кибербезопасность перестаёт быть вспомогательной функцией и превращается в самостоятельное направление экономической деятельности, напрямую связанное с устойчивостью компаний и государств.

Современные организации инвестируют не только в антивирусные решения, но и в системы обнаружения и предотвращения атак, средства защиты облачных сервисов, технологии шифрования, мониторинг инцидентов, а также в обучение сотрудников основам цифровой гигиены и безопасного поведения в информационной среде [11]. Подобные меры позволяют снизить вероятность успешных атак, минимизировать ущерб от возможных инцидентов и повысить общий уровень устойчивости цифровой среды.

Следствием роста внимания к вопросам информационной защиты становится устойчивое увеличение спроса на специалистов в данной сфере. На рынке труда появляются и активно развиваются новые профессиональные направления: аналитики киберугроз, специалисты по защите данных, эксперты по цифровой криминалистике, инженеры информационной безопасности и другие профильные категории работников [6]. Это свидетельствует о том, что кибербезопасность формирует не только технологический, но и кадровый сегмент новой экономики.

Значительную роль в развитии отрасли играют ведущие компании, специализирующиеся на цифровой защите. Среди них можно выделить Kaspersky, Cisco, CrowdStrike и Palo Alto Networks. Эти организации разрабатывают решения для противодействия вредоносным программам, выявления аномальной активности, защиты сетевой инфраструктуры и обеспечения безопасности критически важных систем. Их деятельность демонстрирует, что кибербезопасность сегодня представляет собой высокотехнологичный, наукоёмкий и экономически значимый сектор, влияющий на развитие цифрового общества в целом [13].

**Роль кибербезопасности в обеспечении национальной устойчивости**

Киберугрозы в современных условиях представляют собой значимый риск не только для коммерческих организаций, но и для государства в целом. В условиях цифровой трансформации практически все ключевые сферы общественной жизни и государственного управления — банковский сектор, энергетика, транспорт, здравоохранение и системы связи — в той или иной степени зависят от информационных технологий. Это означает, что устойчивость цифровой инфраструктуры становится одним из важнейших условий нормального функционирования государства [14].

Воздействие на государственные информационные системы может привести к серьёзным последствиям, включая нарушения в работе критически важной инфраструктуры, сбои в банковских операциях, утечку конфиденциальных данных, а также ограничение доступа к транспортным и коммуникационным сервисам. В связи с этим кибербезопасность следует рассматривать не как узкотехническую задачу, а как стратегический элемент обеспечения национальной безопасности и стабильности [5].

Для Республики Узбекистан данная проблема приобретает особую актуальность в условиях последовательного расширения цифровых государственных услуг, развития электронного правительства и внедрения современных информационных систем в сферу управления. По мере роста объёма цифровых данных и увеличения числа онлайн-сервисов возрастает необходимость в создании надёжных механизмов защиты информации, предупреждения инцидентов и минимизации возможного ущерба от кибератак [4].

В этой связи в Узбекистане особое значение приобретают меры по развитию национальной системы киберзащиты, подготовке квалифицированных специалистов, совершенствованию нормативно-правовой базы, а также повышению уровня цифровой грамотности пользователей. Таким образом, кибербезопасность в современных условиях выступает важнейшим условием не только технологического развития, но и устойчивого функционирования государства в целом [1].

В своём Послании Олий Мажлису Президент Республики Узбекистан Шавкат Мирзиёев особо подчеркнул необходимость ускоренного развития цифровой экономики, внедрения современных информационных технологий и укрепления систем кибербезопасности. Глава государства отметил, что защита цифровой инфраструктуры и персональных данных граждан должна стать одним из приоритетных направлений государственной политики, поскольку устойчивое развитие страны напрямую связано с

безопасностью информационного пространства и уровнем цифровой защищённости общества [2].

**Будущее цифровой безопасности.**

Развитие искусственного интеллекта, облачных вычислений и интернета вещей открывает перед обществом и бизнесом новые возможности, однако одновременно усиливает и спектр потенциальных рисков. По мере роста числа подключённых устройств расширяется и поверхность атаки, что делает цифровую среду более уязвимой для киберпреступников [14]. В этих условиях вопросы защиты информации приобретают не эпизодический, а постоянный и системный характер.

В перспективе организации будут вынуждены направлять ещё больше ресурсов на обеспечение безопасности данных, совершенствование защитной инфраструктуры и внедрение интеллектуальных механизмов обнаружения угроз. Особую значимость получат решения, основанные на анализе больших массивов данных, машинном обучении, автоматическом выявлении аномалий, а также на биометрических методах аутентификации [11]. Подобные технологии позволят не только быстрее реагировать на атаки, но и переходить от реактивной модели защиты к проактивной.

Вместе с тем технические средства не могут полностью заменить человеческий фактор. Значительная доля инцидентов по-прежнему связана с ошибками сотрудников, использованием слабых паролей, несоблюдением базовых правил цифровой гигиены и недостаточным уровнем осведомлённости пользователей [7]. Следовательно, повышение цифровой грамотности, формирование культуры ответственного поведения в цифровой среде и регулярное обучение правилам информационной безопасности становятся неотъемлемыми условиями эффективной защиты в современном обществе.

Таким образом, кибербезопасность в XXI веке становится неотъемлемой частью устойчивого развития цифровой экономики и важнейшим условием сохранения стабильности современного общества. Эффективная защита информации требует комплексного подхода, объединяющего технологические решения, государственную поддержку, развитие кадрового потенциала и высокий уровень цифровой культуры пользователей. В условиях стремительного развития технологий именно способность государства и бизнеса своевременно адаптироваться к новым угрозам будет определять уровень их безопасности и конкурентоспособности в будущем [1].

**Заключение**

Проведённый анализ позволяет утверждать, что кибербезопасность в современных условиях представляет собой не вспомогательный, а системообразующий элемент цифровой экономики, обеспечивающий её устойчивость, непрерывность и конкурентоспособность. Усиление зависимости социально-экономических процессов от информационно-коммуникационных технологий закономерно сопровождается ростом масштабов и сложности киберугроз, что, в свою очередь, трансформирует как архитектуру корпоративной защиты, так и государственные подходы к обеспечению информационной безопасности [14]. Следовательно, кибербезопасность следует рассматривать как стратегический ресурс, без которого невозможно эффективное функционирование цифровой инфраструктуры.

Особую значимость в данном контексте приобретают не только технические средства противодействия атакам, но и организационно-экономические механизмы защиты, включая инвестиции в специализированные решения, развитие кадрового потенциала, совершенствование нормативно-правовой базы и формирование национальных стратегий киберзащиты [1]. При этом последствия киберинцидентов выходят далеко за рамки прямых финансовых потерь, поскольку затрагивают

репутационную устойчивость организаций, уровень доверия пользователей, стабильность бизнес-процессов и качество управления данными. Тем самым кибербезопасность становится интегральным условием сохранения экономической и институциональной устойчивости в цифровой среде.

В перспективе роль кибербезопасности будет неуклонно возрастать под влиянием дальнейшего распространения искусственного интеллекта, облачных платформ, интернета вещей и иных цифровых технологий, формирующих новые векторы уязвимости [11]. В этих условиях обеспечение информационной защиты приобретает характер не разовой меры, а непрерывного процесса, предполагающего постоянную адаптацию к меняющимся угрозам и внедрение инновационных механизмов реагирования. Следовательно, цифровая безопасность уже сегодня выступает неотъемлемым основанием новой экономической реальности, в которой информация, её сохранность и защищённость определяют устойчивость развития общества и государства [13].

**Литература**

1. Мирзиёев Ш. М. — Стратегия кибербезопасности Узбекистана на 2026–2030 годы / указ Президента Республики Узбекистан. 2026. Ташкент: официальный источник.
2. Мирзиёев Ш. М. — Послание Президента Республики Узбекистан Олий Мажлису (по вопросам цифровизации и кибербезопасности). 2025. Ташкент: официальный источник.
3. Мусаева А. К. — Цифровизация образования как глобальный тренд. 2025. Бухара: Asian International University / InLibrary.
4. Материалы Центра кибербезопасности Республики Узбекистан — Кибербезопасность и защита цифровой инфраструктуры https://csec.uz/ru/contacts
5. Серебренникова А. В. — Правовые основы кибербезопасности в Российской Федерации. 2021. Москва: МГУ им. М. В. Ломоносова.
6. Матвеев В. А., Цирлов В. Л. — Состояние и перспективы развития индустрии информационной безопасности Российской Федерации. 2013. Журнал «Вопросы кибербезопасности».
7. Бочкарев М. А., Марценюк А. В., Корнилов А. В. — Киберпреступность в условиях современного мира: тенденция развития и методы противодействия. 2019. Журнал «Студенческий вестник», № 46-3 (96).
8. Бирюков А. — Информационная безопасность: защита и нападение. Учебное издание, Москва: ДМК Пресс.
9. Диогенес Ю., Озкайя Э. — Кибербезопасность: стратегии атак и обороны. Москва: Эксмо / учебное издание.
10. Mitnick K., Simon W. L. — The Art of Invisibility. 2017. New York: Little, Brown and Company.
11. Diogenes Y., Ozkaya E. — Cybersecurity: Attack and Defense Strategies. 2018. Birmingham: Packt Publishing.
12. Miller C. — Cybersecurity Essentials. 2020. Indianapolis: Wiley.
13. Schneier B. — Click Here to Kill Everybody: Security and Survival in a Hyper-connected World. 2018. New York: W. W. Norton & Company.
14. World Bank / ITU materials on cybersecurity — Global Cybersecurity Program (international policy and framework materials). Женева: International Telecommunication Union.