Киберпреступность как УГРОЗА цифровой глобализации

УДК 339.1

Аннотация. *Уточнено содержание понятий «киберпреступность» и «киберпреступление», проанализированы основные формы и тенденции преступной деятельности в цифровом пространстве. Рассмотрены ее экономические последствия, разобраны основные положения Глобального индекса кибербезопасности (GCI), программных документов отдельных стран. Предложены меры по совершенствованию системы противодействия киберпреступности в условиях цифровой глобализации, включая развитие национальной системы кибербезопасности, внедрение технологий искусственного интеллекта в работу государственных органов, совершенствование нормативной правовой базы, укрепление международного сотрудничества и развитие кадрового потенциала в этой сфере. Результаты исследования могут быть использованы при разработке государственной политики в области цифровой безопасности и противодействия киберпреступности.*

Ключевые слова: *цифровая глобализация, угрозы цифровой глобализации, киберпреступления, киберпреступность, искусственный интеллект, дипфейки, ИИ-преступления.*

Для цитирования: *Головенчик Г., Головенчик М., Алексеев А. Киберпреступность как угроза цифровой глобализации // Наука и инновации. 2026. №6. С. 37–45.*

https://doi.org/10.29235/1818-9857-2026-06-37-45

Галина Головенчик,
доцент кафедры международных экономических отношений факультета международных отношений Белорусского государственного университета, кандидат экономических наук, доцент; goloventchik@bsu.by

Марина Головенчик,
старший преподаватель кафедры уголовного права юридического факультета Белорусского государственного университета, кандидат юридических наук;
goloventchikmg@bsu.by

Антон Алексеев,
соискатель кафедры экономической информатики Белорусского государственного университета информатики и радиоэлектроники;
alekseev_A@mpt.gov.by

Под киберпреступностью следует понимать совокупность киберпреступлений, совершаемых в цифровом пространстве с помощью или посредством компьютерных систем или сетей против компьютерных систем, сетей или данных. Киберпреступление, в свою очередь, представляет собой общественно опасное деяние с целью нанесения экономического, политического, морального, идеологического, культурного и других видов ущерба индивиду, организации или государству по любым техническим каналам, имеющим доступ к сети Интернет.

Зачастую термин «киберпреступность» используется как синоним компьютерной преступности и преступности в сфере высоких технологий, которым в русскоязычной литературе отдается большее предпочтение.

В связи с развитием ИКТ и их массовым внедрением во все сферы жизнедеятельности в мировой практике получили распространение следующие виды киберпреступлений *(рис. 1)*.

Главная угроза для экономики обусловлена рядом причин, среди них масштабы производимых хакерами атак, их трансграничность, рост профессионализма киберпреступников, а также атак в отношении многочисленных клиентов и кредитных учреждений, незнание и недооценка последними реальных рисков и потенциальных проблем, несоответствие скорости внедрения защитных мер темпам развития киберугроз в финансовом секторе.

Их ландшафт радикально трансформируют стремительная цифровизация экономики, технологии искусственного интеллекта (ИИ) и рост трансграничных цифровых финансовых потоков. В этих условиях обеспечение кибербезопасности приобретает критически важное значение не только для отдельных организаций, но и для глобальной экономической стабильности.

Преступления, совершаемые в цифровом пространстве, отличаются повышенной общественной опасностью в силу длительности их характера. В условиях трансграничности бизнес-процессов кибератака может исходить не от отдельного субъекта преступной деятельности, а от систем искусственного интеллекта, которые в круглосуточном режиме инициируют взлом и вторжение в отношении любых IP-адресов, обнаруживаемых в сети Интернет. Подобные деяния обладают высокой латентностью, а установление лиц, их совершивших, сопряжено с огромными трудностями, что, в свою очередь, препятствует привлечению виновных к юридической ответственности.

Рис. 1. Виды киберпреступлений

Различные экспертные оценки и отчеты авторитетных международных организаций позволяют выделить 8 ключевых тенденций киберпреступности, наблюдаемых в последние годы, и дать их сущностную характеристику, в том числе определив правовое значение *(табл. 1)*.

Анализ экономических последствий киберпреступлений

В отчете Global Cybersecurity Outlook 2026, подготовленном специалистами Всемирного экономического форума, отмечены качественные изменения в характере киберугроз, структуре киберпреступной деятельности и стратегии киберзащит [3]. По его данным, в 2025 г. наблюдался стремительный рост киберпреступлений, основанных на механизмах социальной инженерии. Порядка 77% организаций частного сектора сообщили об увеличении числа случаев кибермошенничества и фишинга, а 73% респондентов указали, что они лично либо через свое ближайшее окружение сталкивались с мошенническими схемами [3]. Это свидетельствует о смещении фокуса киберпреступности от преимущественно технических атак к моделям, эксплуатирующим поведенческие и когнитивные уязвимости пользователей.

Несмотря на сохранение высокой опасности программ-вымогателей, их относительное восприятие различается на уровне управленческих ролей: специалисты по кибербезопасности продолжают рассматривать вредоносные ПО как одну из ключевых технических угроз, тогда как руководители высшего звена в большей степени выделяют финансовые и репутационные риски, связанные с кибермошенничеством. Данное расхождение указывает на изменение приоритетов управления киберрисками в корпоративной практике.

Фиксируется усиление роли ИИ как ключевого технологического драйвера. Как отмечают эксперты, применение этих технологий носит двойственный характер [1, 3]. С одной стороны, генеративные модели используются злоумышленниками для автоматизации фишинговых кампаний, создания правдоподобных сообщений и масштабирования мошен-

Тенденции	Сущностная характеристика	Экономическое и (или) правовое, криминологическое значение	Источники, на которых базируются выводы
Манипулирование доверием граждан для совершения противоправных деяний	Недостаточная кибергигиена и высокая убедительность ИИ-мошенничества	Смещение фокуса с технических уязвимостей на поведенческие	McAfee (2026) [1] Forbes (2025) [2]
Использование технологий ИИ при совершении киберпреступлений	Применение генеративных и агентных ИИ-систем для автоматизации разведки, атак, фишинга и мошенничества Упрощение способов совершения преступлений	Усложнение атрибуции и доказывания вины Рост масштабируемости преступлений	World Economic Forum (2026) [3] Trend Micro (2025) [4] McAfee (2026) [1]
Массовое цифровое мошенничество (онлайн-фрод)	Экспоненциальный рост количества мошеннических сообщений Интеграция мошенничества в повседневную цифровую коммуникацию	Рост частного ущерба Перераспределение издержек на пользователей и бизнес	McAfee (2026) [1]
Активное развитие криптопреступности	Использование криптоактивов и децентрализованных финансовых инструментов в качестве средств и предметов общественно опасных деяний, что обеспечивает трансграничный характер, псевдоанонимность участников и высокую технологическую сложность совершаемых операций	Системные риски для финансовой стабильности, доверия инвесторов и функционирования криптобанков Усложняет квалификацию и доказывание преступлений, повышает требования к ответственности финансовых посредников, включая криптобанки, и требует адаптации международных механизмов уголовно-правового сотрудничества с учетом специфики распределенных реестров	World Economic Forum (2026) [3] Chainalysis (2025) [5]
Массовое создание дипфейков 2.0 как новая реальность киберпреступности	Использование ИИ-сгенерированного контента для обеспечения доверительных коммуникаций с жертвами для совершения преступлений	Подрыв доверия к цифровым институтам	McAfee (2026) [1] Forbes (2025) [2]
Дезорганизация цепочек поставок IT-решений	Несанкционированный доступ к данным пользователей с целью применения в противоправных целях Подрыв деловой репутации поставщиков ПО, сервисов и облачных решений	Эффект «диффузии ответственности» Системный риск для экономики и критических отраслей	Trend Micro (2025) [4]
Геополитизация киберпреступности	Интеграция киберпреступных практик в геополитическое противостояние и гибридные конфликты с размыванием границ между преступной и квази-государственной киберактивностью	Повышение латентности, сетевой организации и повторяемости преступной деятельности, трансформация структуры киберпреступности в сторону устойчивых трансграничных и гибридных форм Увеличение экономических рисков для государств и трансграничного бизнеса	Truesec (2026) [6]
Рост совокупного экономического ущерба	Глобальные потери от киберпреступности оцениваются более чем в 11 трлн долл. в год	Давление на мировую экономику Необходимость системных превентивных мер	Statista (2024) [7]

Таблица 1. Ключевые тенденции киберпреступности

нических операций. До 87% специалистов рассматривают уязвимости, связанные с ИИ, как наиболее быстрорастущую категорию рисков в 2026 г., что свидетельствует о потребности в наличии соответствующих механизмов риск-менеджмента. С другой – искусственный интеллект активно внедряется в системы киберзащиты для обнаружения и реагирования на инциденты. Порядка 94% руководителей считают, что ИИ окажет определяющее влияние на трансформацию кибербезопасности в текущем году. Одновременно наблюдается рост зрелости практик управления рисками. Доля организаций, способных самостоятельно проводить оценку безопасности ИИ-инструментов до их внедрения, увеличилась с 37% в 2025 г. до 64% к началу 2026 г. [3].

Следует также отметить рост рынка киберпреступной деятельности по модели «киберпреступление как услуга», которая снижает порог входа для

новых участников и способствует масштабированию атак. Она функционирует по логике организованного рынка, где вредоносные инструменты, доступы и инфраструктура предлагаются как сервисы, что повышает устойчивость преступной экосистемы.

Один из наиболее уязвимых – финансовый сектор [8, 9], характеризующийся высоким уровнем цифровизации, выражающимся не только в трансформации бизнес-процессов, но и развитии цифровых активов. Это создает благоприятную среду для совершения киберпреступлений и появления все новых их видов. Финансовые институты, имеющие доступ к активам граждан и организаций, а также персональным данным, являются приоритетными целями для злоумышленников.

По данным немецкой бизнес-платформы Statista, 23% всех кибератак в мире в 2024 г. были направлены на эту сферу [8]. Всемирный экономический форум относит ее к критической инфраструктуре [9]. В 2024 г. в ней было зафиксировано 3336 киберпреступлений, что почти в 4 раза выше показателя 2013 г. [10]. Согласно сведениям МВФ, за последние 20 лет совершено более 20 тыс. кибератак на финансовые организации, что повлекло за собой ущерб в размере 12 млрд долл. [11]. По состоянию на конец 2024 г. 67% всех киберпреступлений в мире, совершенных против этого сектора, привели к утечке конфиденциальных данных, 26% – сбоям в работе, 5% – потере финансовых активов [12]. Вышеперечисленные последствия не только негативно влияют на репутацию финансовых структур, но и снижают устойчивость мировой и национальных финансовых систем. Растущее число киберпреступлений влечет за собой необходимость крупных инвестиций в модернизацию систем кибербезопасности, обучение сотрудников.

Особое внимание киберпреступники уделяют цифровым валютам. К 2030 г. ожидается их более широкое внедрение в платежные системы, расчеты по заработной плате и международные финансовые сервисы. Это новая зона киберрисков, связанная с атаками на криптовалютные биржи, кошельки и инфраструктуру блокчейна, включая смарт-контракты.

В отчете ВЭФ представлены примеры масштабных инцидентов, при которых в результате атак на криптоинфраструктуру были утрачены активы на сумму свыше 1,5 млрд долл. [3].

Все это позволяет сделать вывод о том, что современная киберпреступность характеризуется ростом социально-инженерных атак, коммерциализацией преступных моделей и активным внедрением ИИ. В ответ на эти вызовы кибербезопасность развивается в направлении ИИ-ориентированных решений, однако остается подверженной влиянию геополитических факторов и структурного кибернеравенства. К тому же массовое использование цифровых валют усложняет ландшафт угроз, формируя новые требования к защите цифровой финансовой инфраструктуры и государственному регулированию.

Ущерб от киберпреступности включает потери от уничтожения данных, хищения денежных средств, снижения производительности, кражи интеллектуальной собственности, персональных и финансовых сведений, присвоения и мошенничества, сбоев в нормальной хозяйственной деятельности после атак, расходов на судебно-технические расследования, восстановления и удаления скомпрометированных информации и систем, уничтоженной / ухудшенной репутации, судебных издержек и возможных наказаний. За 2025 г. совокупный ущерб от киберпреступности, на основе статистических данных компании Cybersecurity Ventures, достиг 10,5 трлн долл. [13], а это практически равно присутствию теневой «третьей экономики» в мире после США и КНР. Подобные масштабы отражают крупнейшее в истории перераспределение экономического богатства, подрывают стимулы к инновациям и инвестициям, многократно превышают по объему ущерб от природных катастроф за год и превосходят прибыль от мирового оборота всех основных видов незаконных наркотиков в совокупности.

Методологии и рейтинги оценки кибербезопасности стран

Для оценки состояния кибербезопасности существуют несколько международных рейтингов, наиболее авторитетным из которых является Глобальный индекс кибербезопасности (GCI) [14], который выпускается Международным союзом электросвязи с 2015 г. и обновляется раз в 2 года. Он охватывает 172–194 страны и не только оценивает их усилия в этой сфере, но и помогает определить направления повышения уровня кибербезопасности, способствует обмену опытом. GCI интегрирует 20 индикаторов, объединенных по 5 направлениям (технические, правовые и организационные меры, меры в отношении сотрудничества и развития потенциала), и затем суммирует их в общую оценку.

Среди лидеров в 2024 г., относящихся к первому классу индекса (Tier 1 – Role-modelling) из пяти возможных, отражающих статус 172 стран, принимавших

Критерий сравнения	Беларусь	Турция	Интерпретация различий
Общий балл GCI	61,45	100	Турция входит в число мировых лидеров, Беларусь находится в середине рейтинга
Уровень зрелости (Tier)	Уровень 3 (Т3) – базовый	Уровень 1 (Т1) – передовой	Турция демонстрирует всеобъемлющую и зрелую систему кибербезопасности, Беларусь – базовый уровень кибербезопасности
Правовые меры	18,61	20	Турция демонстрирует максимальный результат, что отражает зрелое национальное законодательство в сфере кибербезопасности, гармонизированное с лучшими международными стандартами. Беларусь имеет развивающуюся правовую базу, что указывает на продолжающийся процесс формирования и имплементации правовой базы
Технические меры	2,78	20	Наибольший разрыв: у Турции – развитая индустрия кибербезопасности, у Беларуси существует разрыв между нормативным закреплением мер и их практической технологической реализацией на национальном уровне
Организационные меры	11,97	20	Турция демонстрирует эффективные стратегии и оперативные возможности, у Беларуси показатель отражает прогресс в организационном строительстве, но указывает на потенциал для укрепления координации и операционной эффективности
Меры по наращиванию потенциала	8,98	20	Турция обладает признанной на мировом уровне экосистемой подготовки кадров и R&D в области кибербезопасности. В Беларуси имеется образовательный потенциал, но требуется большая связь с практическими нуждами, а также развитие программ повышения осведомленности
Меры сотрудничества	19,11	20	Обе страны демонстрируют высокие результаты. Турция и Беларусь успешно интегрированы в систему международного диалога и сотрудничества по кибербезопасности, что является их сильной стороной

Таблица 2. Сравнительный анализ Беларуси и Турции по Глобальному индексу кибербезопасности (GCI, 2024)

Примечание: авторская разработка на основе Global Cybersecurity Index 2024 [14]

участие в оценке, отмечены 47 (оценка в диапазоне 95–100), в том числе Австралия, Бахрейн, Бангладеш, Бельгия, Бразилия, Кипр, Дания.

В рейтинге GCI 2020 [15] Беларусь заняла 89-е место из 194 стран, но уже в GCI 2024 она улучшила общий балл с 50,57 до 61,45 и была отнесена к странам 3-го уровня (Т3), демонстрируя базовую приверженность обеспечению кибербезопасности посредством принятия государственных мер [14]. Однако анализ отдельных субиндексов указывает на существующие и довольно значительные дисбалансы. В частности, высокие баллы получены за «Меры сотрудничества», включая участие в международных соглашениях, и «Правовые меры». Довольно низкие показатели нашей страны отмечены в компоненте «Технические меры».

Принятие в 2023 г. Указа Президента Республики Беларусь №40 «О кибербезопасности», который заложил основы для создания национальной системы противодействия киберугрозам, позволило значительно улучшить показатель «Правовые меры» по сравнению с 2020 г. [16]. Тем не менее слабость технической реализации демонстрирует разрыв между нормативным закреплением и практическими технологическими возможностями.

Для более глубокого понимания позиций и вызовов в области кибербезопасности проведем сравнительный анализ государств – лидеров в данной сфере. В качестве референтного государства выбрана Турция, стабильно входящая в первую десятку мирового рейтинга GCI и признанная одним из глобальных центров кибербезопасности. Согласно данным GCI 2024, Турция относится к странам 1-го (наивысшего) уровня (Т1) зрелости в общемировом рейтинге с результатом 100 баллов.

Детальное сопоставление показателей по 5 ключевым компонентам индекса выявляет структурные различия двух стран. Систематизированный сравнительный анализ приведен в *табл. 2*.

Сопоставление с одной из сильнейших моделей в области кибербезопасности показывает, что основное отличие Беларуси от Турции заключается не в формальном наличии мер (где в Беларуси уже достигнут значительный прогресс), а в их качественной технологической реализации и масштабах национальной индустрии кибербезопасности. Опыт Турции подчеркивает важность тесной взаимосвязи между передовыми исследованиями, коммерческими разработками, подготовкой элитных кадров и государственными нуждами. Для Беларуси,

обладающей сильным IT-образовательным фундаментом, стратегическим приоритетом должно стать направление этого потенциала на развитие внутреннего рынка киберрешений и технологического суверенитета, что позволит не только подняться в рейтингах, но и существенно повысить устойчивость национальной цифровой экосистемы.

Относительно стран Содружества Независимых Государств отметим, что Беларусь уступает лидерам региона – Казахстану и России (уровень 2 – Advancing), но находится выше других государств – членов СНГ.

Меры по противодействию киберпреступности

Большинство стран мира приняли государственные стратегии кибербезопасности (или их новые редакции), анализ которых с позиции GCI дан в *табл. 3*.

Следует также отметить, что во многих государствах 4-го и 5-го уровня GCI отсутствуют отдельные стратегии кибербезопасности, что, по нашему мнению, затрудняет борьбу с киберпреступностью.

Исходя из проведенного анализа можно сделать вывод о наличии ярко выраженного кибернеравенства между мировыми регионами. Различия в доступе к ресурсам, компетенциям и технологиям приводят к тому, что уровень готовности к серьезным киберинцидентам остается неравномерным, особенно в развивающихся регионах, включая страны Латинской Америки и Карибского бассейна. Данная асимметрия усиливает системные риски, что подчеркивает необходимость международного сотрудничества в сфере киберустойчивости.

Усилия Республики Беларусь по кибербезопасности

Наша страна прилагает значительные усилия в сфере противодействия киберпреступлениям. В 2023 г. в Следственном комитете Республики Беларусь (СК) было создано Главное управление

Страна, уровень в GCI	Наименование документа, год принятия и источник	Основные направления и цели
США (1)	President Trump's Cyber Strategy for America (2026) [17]	Разрушение криминальных сетей, усиление ответственности правонарушителей Упрощение бюрократических норм, приоритет защиты приватности данных американцев Внедрение zero-trust архитектуры, постквантовой криптографии, инструментов ИИ и облачных решений Усиление защиты энергетического комплекса, финансового сектора, здравоохранения Обеспечение безопасных цепочек поставок, поддержка ИИ, криптовалют и квантовых вычислений с акцентом на инновации Создание системы подготовки киберспециалистов Цели: активное противодействие киберугрозам, укрепление технологического лидерства США, обеспечение свободы и безопасности в Интернете, а также снижение экономического ущерба от атак
Дания (1)	The Danish Government's National Strategy for Cyber and Information Security 2022–2024 (2021) [18]	Укрепление национальной киберзащиты, повышение устойчивости инфраструктуры, развитие сотрудничества государственно-частного сектора, борьба с киберпреступностью, международное партнерство Цели: повышение осведомленности, стандартизация мер, защита ключевых секторов (энергия, финансы)
Китай (2)	National Cyberspace Security Strategy (2016, с обновлениями) [19]	Киберсуверенитет, локализация данных, защита критической инфраструктуры (CII), многоуровневая система защиты (технологии + законы), развитие отечественных технологий Цели: реализация концепций инноваций, координации, «зеленого» развития, открытости и совместного использования в рамках общей концепции национальной безопасности, повышение осведомленности о рисках и кризисах, координация внутренних и внешних ситуаций, балансировка задач развития и безопасности с целью активной защиты и эффективного реагирования на вызовы, продвижение мирного, безопасного, открытого, кооперативного и упорядоченного киберпространства, обеспечение суверенитета, безопасности и интересов развития страны для построения кибервеликой державы
Россия (2)	Доктрина информационной безопасности Российской Федерации (2016) [20]	Защита суверенитета в информационной сфере, безопасность критической информационной инфраструктуры, импортозамещение, государственно-частное партнерство Цели: формирование государственной политики, развитие общественных отношений и выработка мер по совершенствованию системы

Страна, уровень в GCI	Наименование документа, год принятия и источник	Основные направления и цели
Беларусь (3)	Концепция информационной безопасности (2019) [21]	Мониторинг угроз, безопасность СМИ и государственных сервисов, информационный суверенитет и нейтралитет, защита инфо-инфраструктуры, государственно-частное партнерство, международное сотрудничество Цели: создание методологической основы для совершенствования деятельности по укреплению информационной безопасности, формирование государственной политики, выработка мер по совершенствованию системы обеспечения информационной безопасности, конструктивного взаимодействия, консолидации усилий и повышения эффективности защиты национальных интересов в информационной сфере
Новая Зеландия (3)	New Zealand's Cyber Security Strategy 2026–2030 (2026) [22]	Повышение осведомленности о рисках, улучшение отчетности об инцидентах, обмен информацией между правительством и бизнесом Управление рисками для критической инфраструктуры, регулирование, модернизация правительственных систем, подготовка к постквантовой эре Эффективный отклик на инциденты, модернизация законодательства для противодействия угрозам, включая киберпреступность Укрепление сотрудничества с государствами мира Цели: создание устойчивого общества через понимание рисков, , предотвращение ущерба, эффективный отклик на инциденты и стратегическое партнерство
Сальвадор (4)	Política de Ciberseguridad de El Salvador	Институциональное и нормативно-правовое укрепление системы кибербезопасности, развитие механизмов предупреждения и реагирования на киберинциденты, повышение уровня цифровой осведомленности и компетенций, управление киберрисками, а также расширение межсекторного и международного сотрудничества Цели: формирование устойчивого и защищенного национального киберпространства посредством координации государственных и негосударственных акторов, снижение уязвимостей критической цифровой инфраструктуры, обеспечение правового и организационного противодействия киберугрозам и повышения общей киберустойчивости государства и общества
Лихтенштейн (4)	National Strategy For Protection Against Cyber Risks (2025) [24]	Последовательное развитие национального уровня киберустойчивости через расширение осведомленности и взаимодействия всех социальных и экономических акторов, укрепление защиты критически важных инфраструктур и финансового сектора, обеспечение кооперации между государственными и частными субъектами, а также создание механизмов предупреждения и преодоления кризисных ситуаций, что отражает мультидисциплинарный и институционально согласованный подход к кибербезопасности Цели: обеспечение всестороннего понимания киберрисков всеми ключевыми участниками, повышение их устойчивости к угрозам и способность к адаптивному реагированию, формирование сетевого сотрудничества внутри страны и за ее пределами, а также стимулирование ответственного участия всех заинтересованных сторон в разработке и реализации мер по снижению воздействия киберинцидентов
Афганистан (5)	National Cyber Security Strategy of Afghanistan (2014) [25]	Развитие институциональных механизмов защиты государственных информационных и коммуникационных систем через создание и усиление координационных структур, повышение технических и организационных возможностей для предупреждения и реагирования на киберугрозы, формирование нормативно-правовой базы и развитие партнерства между государственным и частным секторами, адаптация международных стандартов и лучшей практики в интересах устойчивой цифровой среды Цели: обеспечение надежной защиты критической информационной инфраструктуры, повышение национального потенциала по предотвращению, обнаружению и реагированию на киберинциденты, укрепление правовой и институциональной структуры для безопасного функционирования государственных и частных цифровых систем, а также стимулирование международного сотрудничества в области защиты данных и борьбы с киберпреступностью
Мальдивы (5)	The National Cyber Security Strategy (NCSS) for 2024–2029 (2024) [26]	Формирование комплексного управления киберрисками, укрепление технологической и организационной устойчивости, развитие внутреннего потенциала и осведомленности сотрудников, интеграция безопасных процессов и практик защиты информационных систем, а также укрепление нормативных функций и сотрудничества между финансовыми институтами и государственными структурами Цели: защита национальных и общественных интересов посредством обеспечения безопасности информационных систем от киберугроз, повышение уровня киберустойчивости за счет развития способности к восстановлению после инцидентов, укрепление международного и регионального лидерства через достижение признания на глобальном уровне, создание условий для экономического роста посредством формирования безопасной цифровой среды, а также межсекторного и межгосударственного сотрудничества

Таблица 3. Государственные стратегии (концепции) кибербезопасности отдельных стран уровней 1–5 индекса GCI

цифрового развития предварительного следствия, которое обеспечивает информатизацию служебной деятельности, реализацию единой цифровой политики, координацию разработки информационных систем, а также играет ключевую роль в противодействии киберпреступности; в поддержку этих задач сформированы специализированные региональные подразделения, образующие самостоятельную подсистему в структуре СК.

В обеспечении кибербезопасности также участвуют Комитет государственной безопасности Республики Беларусь, Генеральная прокуратура, Оперативно-аналитический центр при Президенте. Кроме того, данным вопросам уделяется особое внимание со стороны финансовых институтов, контролирующих обмен данными через автоматизированные системы для блокировки противоправных финансовых операций. Так, Национальный банк активно реализует меры по противодействию киберпреступлениям, включая утверждение стандартов информационной безопасности и взаимодействие с банками и правоохранителями. Еще в 2019 г. были приняты Концепция обеспечения кибербезопасности в банковской сфере и план мер по ее реализации, нацеленные на создание единой системы защиты, совершенствование управления киберрисками и укрепление взаимодействия между банками [27]. С 2023 г. действует Указ Президента Республики Беларусь от 29.08.2023 г. №269 «О мерах по противодействию несанкционированным платежным операциям», направленный на противодействие мошенничеству в банковской сфере и обеспечение взаимодействия граждан, органов внутренних дел и банковского сектора, в том числе посредством функционирования специализированных дежурных служб в круглосуточном режиме [28]. Он позволил оперативно передавать информацию о противоправных операциях, а также получать данные о лицах и инструментах, задействованных в преступной деятельности, что способствует принятию эффективных мер по сохранению и возврату похищенных денежных средств. С 1 июля 2026 г. обязательны для применения банками антифрод-система при оценке совершаемых операций и цифровой отпечаток устройства [29].

По нашему мнению, назрела необходимость внедрения ИИ для внутреннего использования в государственных структурах, включая Национальный банк Республики Беларусь и правоохранительные органы, что повысит уровень противодействия киберпреступлениям, особенно кибермошенничеству, так как рост атак на финансовый сектор (с 177 инцидентов в 2024 г. до почти 600 за 10 месяцев 2025 г. [30]) демонстрирует пределы применения «традиционных» методов. Простой компьютерный анализ не справляется с большими объемами данных и новыми схемами, такими как NFC-мошенничество, и новыми инвестиционными пирамидами. Применение технологий ИИ обеспечит автоматизированный мониторинг транзакций в реальном времени, поведенческий анализ и предиктивное прогнозирование угроз, интегрируясь с существующими системами типа BlackList АСОИ и антифрод-платформами, что позволит предотвратить совершение противоправных деяний.

Обозначим основные выводы и рекомендации по противодействию киберпреступлениям в условиях Республики Беларусь.

Во-первых, для государств – участниц ЕАЭС необходим собственный инструментарий оценки адаптации стран к цифровой глобализации, который должен включать в себя и субиндекс кибербезопасности, отражающий реальный ущерб как государственным предприятиям, так и частным компаниям и гражданам, что будет способствовать быстрому сбору информации и кооперации внутри интеграционного союза.

Во-вторых, в связи с высокими темпами трансформации способов совершения киберпреступлений необходимо обеспечить оперативное реагирование на них в том числе со стороны правотворческих органов. Так, по мнению авторов, следует внести изменения и дополнения в Концепцию информационной безопасности Республики Беларусь [21] о порядке противодействия киберпреступлениям с использованием технологий ИИ, так как она является основополагающей в Государственной программе «Цифровая Беларусь» на 2026–2030 гг. [31]. В ближайшие годы следует разработать национальные стандарты ИИ-безопасности, что значительно усилит киберустойчивость государства, а также снизит общий уровень киберпреступлений.

В-третьих, необходимо развитие безопасной инфраструктуры, оперативного реагирования на киберугрозы и создание технологий искусственного интеллекта для внутренних нужд правоохранительных органов дружественных стран для обеспечения кибербезопасности региона.

В-четвертых, учитывая, что навыки в области сетевых технологий и кибербезопасности входят в тройку наиболее быстро развивающихся компетенций, спрос на которые, как прогнозируется, существенно возрастет к 2030 г. [32], жизненно важно

целенаправленное повышение квалификации и непрерывное профессиональное обучение в данной области. Намеченное создание специализированного университета для одаренной молодежи всех специальностей требует включения в него программы освоения компетенций по обеспечению кибербезопасности на макро- и микроуровнях.

Статья поступила в редакцию
15.04.2026 г.

Summary. The definitions of the terms «cybercrime» and «cyberoffense» have been clarified, and the main forms and trends of criminal activity in the digital space have been analyzed. The paper examines its economic implications and analyzes the key provisions of the Global Cybersecurity Index (GCI) and the policy documents of individual countries. Measures have been proposed to improve the system for combating cybercrime in the context of digital globalization, including the development of a national cybersecurity system, the implementation of artificial intelligence technologies in the work of government agencies, the improvement of the regulatory framework, the strengthening of international cooperation, and the development of human resources in this field. The results of the study can be used in the development of public policy in the field of digital security and combating cybercrime.

Keywords: digital globalization, threats to digital globalization, cybercrime, artificial intelligence, deepfakes, AI-crime.

https://doi.org/10.29235/1818-9857-2026-06-37-45

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. State of the Scamiverse / McAfee // https://www.mcafee.com/blogs/wp-content/uploads/2026/01/Scamiverse.pdf.
2. The 7 Cyber Security Trends Of 2026 That Everyone Must Be Ready For // Forbes // https://www.forbes.com/sites/bernardmarr/2025/09/26/the-7-biggest-cybersecurity-trends-of-2026-that-everyone-must-be-ready-for.
3. Global Cybersecurity Outlook 2026 // World Economic Forum // https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2026.pdf.
4. Trend Micro Predicts 2026 as the Year Cybercrime Becomes Fully Industrialized / Trend Micro // https://newsroom.trendmicro.com/2025-11-25-Trend-Micro-Predicts-2026-as-the-Year-Cybercrime-Becomes-Fully-Industrialized.
5. The Chainalysis 2025 Crypto Crime Report / Chainalysis // https://go.chainalysis.com/2025-Crypto-Crime-Report.html.
6. Truesec Threat Intelligence Report 2026: AI and Geopolitics Reshape Cyber Risk / Truesec // https://www.truesec.com/news/truesec-threat-intelligence-report-2026-ai-and-geopolitics-reshape-cyber-risk.
7. Estimated cost of cybercrime worldwide 2018–2029 / Statista // https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide.
8. Distribution of cyberattacks across worldwide industries in 2024 / Statista // https://www.statista.com/statistics/1315805/cyber-attacks-top-industries-worldwide/?srsltid=AfmBOoqV5TKlVs5TnGjHP4OGncDwsyfmDjsiodAGmslu-cAEocFomHTB.
9. These sectors are top targets for cybercrime, and other cybersecurity news to know this month / World Economic Forum // https://www.weforum.org/stories/2024/04/cybercrime-target-sectors-cybersecurity-news.
10. Number of cyber incidents in the financial industry worldwide from 2013 to 2024 / Statista // https://www.statista.com/statistics/1310985/number-of-cyber-incidents-in-financial-industry-worldwide.
11. Rising Cyber Threats Pose Serious Concerns for Financial Stability / IMF // https://www.imf.org/en/blogs/articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability.
12. Cyberthreats to the financial sector: forecast for 2025–2026 / Positive Technologies // https://global.ptsecurity.com/en/research/analytics/cyberthreats-to-the-financial-sector-forecast-for-2025-2026.
13. Cybercrime To Cost The World $12.2 Trillion Annually By 2031 / Cybercrime Magazine // https://cybersecurityventures.com/official-cybercrime-report-2025.
14. Global Cybersecurity Index 2024 / ITU // https://www.itu.int/epublications/publication/global-cybersecurity-index-2024.
15. Global Cybersecurity Index 2020 / ITU // https://www.itu.int/hub/publication/d-str-gci-01-2021.
16. О кибербезопасности: Указ Президента Республики Беларусь от 14.02.2023 г. №40 // ilex: информ. правовая система.
17. President Trump's Cyber Strategy for America: the White House, March 2026 // https://www.whitehouse.gov/wp-content/uploads/2026/03/President-Trumps-Cyber-Strategy-for-America.pdf.
18. The Danish National Strategy for Cyber and Information Security 2022–2024: The Danish Government, December 2021 // https://en.digst.dk/media/bxxcnby2/digst_ncis_2022-2024_uk.pdf.
19. National Cyberspace Security Strategy: the State Internet Information Office, the State Internet Information Office, 27 December 2016 // https://www.cac.gov.cn/2016-12/27/c_1120195926.htm.
20. Доктрина информационной безопасности Российской Федерации: Указ Президента Российской Федерации от 05.12.2016 г. №646 // https://base.garant.ru/71556224/#block_2.
21. Концепция информационной безопасности Республики Беларусь: постановление Совета Безопасности Республики Беларусь от 18.03.2019 г. №1 // ilex: информ. правовая система.
22. New Zealand's Cyber Security Strategy 2026–2030: New Zealand Government, February 2026 // https://www.dpmc.govt.nz/publications/new-zealands-cyber-security-strategy-2026-2030.
23. Politica de Ciberseguridad de El Salvador: Secretaría de Innovación de la Presidencia, Abril 2021 // https://database.cyberpolicyportal.org/api/files/1676835572099l9pucn6luha.pdf.
24. National Strategy For Protection Against Cyber Risks: The National Cyber Security Unit of the Principality of Liechtenstein, February 2025 // https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/LI_NCSS_2025_en.pdf.
25. National Cyber Security Strategy of Afghanistan: Ministry of Communications and IT, November 2014 // https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Afghanistan_2014_National%20Cybersecurity%20Strategy%20of%20Afghanistan%20%28November2014%29.pdf.
26. The National Cyber Security Strategy (NCSS) for 2024–2029 National Cyber Security Agency Republic of the Maldives // https://hub.ncsa.gov.mv/strategy.
27. Концепция обеспечения кибербезопасности в банковской сфере и плане мер по ее реализации: постановление Правления Национального банка Республики Беларусь от 20.11.2019 г. №466 // ilex: информ. правовая система.
28. О мерах по противодействию несанкционированным платежным операциям: Указ Президента Республики Беларусь от 29.08.2023 г. №269 // ilex: информ. правовая система.
29. Белорусские банки до 1 июля внедрят новые стандарты для защиты от мошенников // Pravo.by // https://pravo.by/novosti/obshchestvenno-politicheskie-i-v-oblasti-prava/2026/february/92306.
30. Нацбанк фиксирует рост кибератак на финансовые организации // БелТА // https://belta.by/economics/view/natsbank-fiksiruet-rost-kiberatak-na-finansovye-organizatsii-749849-2025.
31. О Государственной программе «Цифровая Беларусь» на 2026–2030 гг.: постановление Совета Министров Республики Беларусь от 30.12.2025 г. №793 // ilex: информ. правовая система.
32. The Future of Jobs Report 2025 / World Economic Forum // https://www.weforum.org/publications/the-future-of-jobs-report-2025.