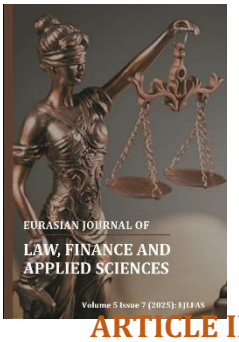
EURASIAN JOURNAL OF LAW, FINANCE AND APPLIED SCIENCES
Innovative Academy Research Support Center
IF = 9.2 www.in-academy.uz/index.php/ejlfas



CRIMINOLOGICAL CHARACTERISTICS OF CYBERCRIME AND PRIORITY AREAS FOR COMBATING IT

Muzaffar Ziyodullaevich Ziyodullaev
Doctor of Juridical Science (DSc), Professor
Tashkent International University
Tashkent, Uzbekistan
e-mail: muzzziyo@gmail.com
https://doi.org/10.5281/zenodo.19331261

ARTICLE INFO

Received: 24th March 2026
Accepted: 29th March 2026
Online: 30th March 2026

KEYWORDS

Cybercrime, cybersecurity, cyber fraud, cyber victim, cyberspace, cyber literacy, transboundary nature, anonymity, artificial intelligence, combating cybercrime, cybercrime prevention.

ABSTRACT

This article provides a systematic analysis of the legal nature of the "cybercrime" phenomenon and its specific features in the context of modern digital transformation. The study classifies the psychological, victimological, technological, economic, and legal factors that contribute to the emergence of crime in cyberspace, and puts forward conceptual proposals for improving the legal regulation of this sphere and its preventive mechanisms.

КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА КИБЕРПРЕСТУПЛЕНИЙ И ПРИОРИТЕТНЫЕ НАПРАВЛЕНИЯ БОРЬБЫ С НИМИ

Музаффар Зиёдуллаевич Зиёдуллаев
доктор юридических наук (DSc), профессор
Tashkent International University Ташкент, Узбекистан
e-mail: muzzziyo@gmail.com
https://doi.org/10.5281/zenodo.19331261

ARTICLE INFO

Received: 24th March 2026
Accepted: 29th March 2026
Online: 30th March 2026

KEYWORDS

Киберпреступление, кибербезопасность, кибермошенничество, кибержертва, киберпространство, киберграмотность, трансграничность, анонимность, искусственный интеллект, борьба с киберпреступлениями,

ABSTRACT

В статье проводится системный анализ правовой природы феномена «киберпреступлений» и его специфических особенностей в условиях современной цифровой трансформации. В ходе исследования классифицируются психологические, виктимологические, технологические, экономические и правовые факторы, способствующие возникновению преступлений в киберпространстве, а также выдвигаются концептуальные предложения по совершенствованию правового регулирования данной сферы и превентивных механизмов.

предупреждения киберпреступлений.

На сегодняшний день переход общества на новый этап развития – информационную и киберразвитую эпоху – обусловил внедрение цифровых технологий во все сферы человеческой жизни. Однако этот процесс приносит с собой не только удобства, но и серьезные угрозы в виде киберпреступности. Проблема борьбы с киберпреступлениями выходит на передний план не только на национальном уровне в каждой отдельной стране, но и в глобальном масштабе. Как справедливо отмечает С.А. Стяжкина, специфика данной проблемы заключается в её многогранности и взаимосвязи с различными факторами. Для эффективного противодействия киберпреступности требуется объединение усилий специалистов в правовой, технической, психологической и социальной областях. Следовательно, согласно статистическим данным, сегодня киберпреступления занимают значительную долю в общей структуре преступности. Например, в России киберпреступления составляют более четверти от общего числа всех преступлений (26,6%) [1]. Согласно криминологическому анализу Х.А. Аккаевой, киберпреступность эволюционировала от простого «фрикинга» (несанкционированного доступа к телекоммуникационным системам) 1970-х годов до высокодоходной сферы «теневой экономики», приносящей сегодня миллиарды долларов убытков. По прогнозам Cybersecurity Ventures, одной из ведущих мировых исследовательских компаний в области кибербезопасности, к 2025 году ежегодный мировой ущерб от киберпреступности достигнет 10,5 триллионов долларов США [2].

В Узбекистане также наблюдается ежедневный рост киберпреступности, при этом количество её видов увеличилось с 18 до 62. В частности, набирают обороты такие виды правонарушений, как кража персональных данных, использование искусственного интеллекта для имитации голоса и человеческого облика (дипфейки), а также распространение вредоносных файлов. Так, за последние шесть лет количество обращений по фактам киберпреступлений в стране выросло в 48 раз. В прошлом году 82 процента мошенничеств и 76 процентов краж были совершены в киберпространстве. Причиненный физическим и юридическим лицам материальный ущерб превысил 2 триллиона сумов. Присвоенные денежные средства выводятся за рубеж в форме криптовалюты. Особенно прискорбным является тот факт, что 95% синтетических наркотиков распространяются через интернет, а расчеты за них производятся исключительно в криптовалюте [3].

Итак, что же такое «киберпреступления» и в чем проявляются их основные особенности? Какие факторы порождают и подпитывают киберпреступность? И какие меры необходимо предпринять для борьбы с киберпреступлениями и их эффективного предупреждения?

Согласно Будапештской конвенции Совета Европы №185 «О киберпреступности» от 23 ноября 2001 года, в узком смысле «*киберпреступность* – это противоправные деяния, совершаемые посредством электронных операций против безопасности компьютерных систем и данных». В широком же смысле она охватывает «любое незаконное деяние, совершенное с использованием компьютерных систем или сетей либо в связи с ними, включая незаконное владение информацией и её распространение» [4].

Согласно рекомендациям экспертов ООН, термин «киберпреступность» охватывает любое преступление, которое может быть совершено с помощью компьютерной системы или сети, в их рамках или против них [5]. По мнению Т.Л. Тропиной, приведенное определение близко к понятию «компьютерная преступность», однако данная категория не может полностью охватить все деяния, совершаемые с помощью вычислительной техники. Она определяет киберпреступность как совокупность преступлений, совершаемых в киберпространстве с помощью компьютерных систем или сетей, а также направленных против них [6].

В связи с этим в литературе по информационному праву приводится следующее определение: «Киберпреступность – это не просто использование техники, а совокупность общественно опасных деяний в виртуальном пространстве с применением информационных технологий, угрожающих информационной безопасности, а также интересам личности, общества и государства» [7].

Понятие «киберпреступность» является более широким и общим по отношению к термину «киберпреступления», оно представляет собой не просто их механическую совокупность, а сложную систему, определяющую их качественные и количественные показатели.

Основываясь на анализе вышеизложенных и иных определений из юридической литературы, мы считаем возможным дать следующее определение понятию «киберпреступления»: «*Киберпреступления* – это совокупность запрещенных уголовным законодательством общественно опасных деяний, направленных против конфиденциальности, целостности и доступности компьютерных данных, а также информационной безопасности личности, общества и государства, совершаемых с использованием информационных технологий и цифровых систем в качестве орудия преступления».

Наиболее распространенным видом киберпреступлений является кибермошенничество.

Р.Р. Кильметова и её соавторы характеризуют явление фишинга (phishing) как одну из наиболее опасных форм мошенничества. Фишинг – это действия, направленные на получение персональных данных пользователей (логинов, паролей, номеров банковских карт) путём обмана. Выделяются следующие его виды: классический фишинг – массовая рассылка сообщений по электронной почте; целевой (spear) фишинг – атака, направленная на конкретное лицо или организацию после предварительного сбора данных о них; смишинг и вишинг – обман, осуществляемый через SMS-сообщения или телефонные звонки [8]. Ряд российских ученых-юристов, изучив подобные киберпреступления на примере опыта России и Китая, пришли к выводу, что во многих случаях нормы уголовных кодексов не проводят четкой границы между мошенничеством и кражей, что создает трудности в правоприменительной практике в данной сфере [9].

Одной из относительно новых форм киберпреступности является *кибербуллинг* – намеренное агрессивное поведение в отношении жертвы, осуществляемое систематически с помощью интернет-платформ (социальных сетей, онлайн-игр, чатов). К формам кибербуллинга относятся: психологический террор, шантаж, непристойные шутки, клевета, бойкот, домогательства и др. Подобное воздействие может привести к крайне тяжелым последствиям для личности, вплоть до совершения самоубийства [10].

В целом, существует множество видов киберпреступлений, и взгляды ученых на этот счет также разнятся. В частности, британские исследователи, такие как К. Филлипс и Дж.К. Дэвидсон, разделяют киберпреступления на две крупные категории: *киберзависимые преступления* – хакерство, DDoS-атаки, распространение вредоносного программного обеспечения; *кибервспомогательные преступления* – кибермошенничество, киберкражи, киберпреследование [11]. Российский исследователь М.Н. Головко, опираясь на опыт зарубежных стран, группирует киберпреступления следующим образом: крипто-мошенничество, фишинг и кража данных, а также манипулирование рынком [12].

По нашему мнению, более широким подходом к классификации киберпреступлений обладают взгляды ученых Университета Аль-Кудс – М. Ахмеада, Н. Аль-Шарифа и И. Абуирама. Они разделяют киберпреступления на следующие категории: *преступления против личности*: кибербуллинг, киберпреследование (cyberstalking), распространение порнографии, секстинг и сексторшн (шантаж с использованием сексуального контента); *преступления против собственности*: кибермошенничество, преступления, связанные с кредитными картами, кража интеллектуальной

собственности; *преступления против государства*: кибертерроризм и атаки на государственные информационные системы [13].

Говоря о специфических особенностях киберпреступлений, в проведенных исследованиях выделяются следующие ключевые характеристики, отличающие их от традиционных преступлений:

1) трансграничность (отсутствие границ) – это важнейшая черта киберпреступности. Преступник может находиться на одном континенте, преступное деяние совершаться на другом, а последствия проявляться в третьем государстве. Благодаря глобальной сети расстояние между преступником и жертвой не имеет значения;

2) высокий уровень латентности (скрытости) – по различным причинам большинство киберпреступлений остаются незарегистрированными. Анализ показывает, что в России уровень латентности преступлений в киберпространстве достигает 85–97%. Это связано с тем, что потерпевшие либо не обращаются в правоохранительные органы, либо вовсе не замечают совершенного преступления [14];

3) анонимность и дистанционность – преступники имеют возможность скрывать свою личность и совершать преступления без вступления в физический контакт. Анализируя особенности киберпреступлений, Н.Д. Гомонов выделяет анонимность глобальной сети и коммуникации вне контроля государственных институтов как основные криминогенные факторы. По его мнению, в киберпространстве традиционные социальные институты не могут в полной мере выполнять свои функции, в результате чего пользователи выходят из-под нормативного контроля [15];

4) интеллектуальный характер и профессионализм – киберпреступники зачастую являются высокообразованными лицами с глубокими знаниями в сфере ИТ, постоянно повышающими свою квалификацию. Они предлагают свои услуги традиционным преступным группам, становясь частью организованной преступности. Следует особо отметить, что у киберпреступников сформировалась специфическая субкультура и возник собственный жаргон – «сленг», понятный только в их узком кругу [16];

5) динамическая изменчивость, автоматизация и консолидация сил – методы совершения преступлений постоянно обновляются, адаптируясь к развитию технологий. Преступники получают возможность автоматизировать процессы и осуществлять множество атак одновременно.

Особую тревогу вызывает тот факт, что интеграция современных информационных технологий с искусственным интеллектом (ИИ) существенно повышает риски киберпреступности. Рут Вандхёфер, старший советник Лондонской фондовой биржи (LSEG), рассуждая о новой эре угроз автономного ИИ, отмечает, что в последнее время

хакеры осваивают искусственный интеллект быстрее, чем бизнес. По её данным, количество атак с использованием программ-вымогателей (ransomware) – когда данные пользователя или вся компьютерная система блокируются с целью получения выкупа за их восстановление – увеличилось на 60%. Среди пострадавших значатся крупные бренды, банки и даже ведущие оборонные организации. Нападавшие начали массово использовать ИИ для автоматизации фишинга и создания глубоких подделок (дипфейков). По её мнению, опасения в этой сфере усиливаются из-за следующих факторов: появление систем, способных самостоятельно выполнять сложные операции без вмешательства человека; снижение надежности традиционных методов аутентификации личности; непреднамеренная передача сотрудниками конфиденциальных корпоративных данных в открытые алгоритмы; рост Onchain-киберпреступности, при которой преступники всё чаще атакуют DeFi-платформы (децентрализованные финансовые сервисы без участия банков или государства) и переносят свою инфраструктуру в блокчейн для уклонения от ответственности; стремление к созданию квантовых компьютеров, обладающих потенциалом для взлома классических методов шифрования [17].

Изучение причин и факторов киберпреступности является одним из наиболее актуальных вопросов современной криминологии и информационной безопасности. Научные исследования показывают, что данные преступления – это не просто технические или технологические сбои, а продукт сложных системных проблем.

Факторы, порождающие киберпреступность, можно классифицировать и изучать следующим образом:

Психологические факторы. Исследования показывают, что из-за отсутствия непосредственного контакта между преступником и жертвой в киберпространстве совершение преступления становится психологически более легким. Виртуальные объекты и действия кажутся «нереальными». Это порождает безответственность, особенно среди молодежи, в отношении требований информационной безопасности и нарушений авторских прав. Поскольку преступник не видит наносимый ущерб своими глазами, чувство вины и ответственности у него притупляется.

Как справедливо отмечает Нэнси Уиллард, директор Центра безопасного и ответственного использования Интернета и известный американский эксперт в области кибербезопасности: «Информационно-коммуникационные технологии значительно ограничивают обратную связь – любое ощутимое чувство последствий наших действий. Поэтому на нас не действует осознание того, что мы причинили вред; мы также полагаем, что наше

поведение не может нанести никакого ущерба, поскольку мы этого ущерба не видим» [18].

Профессор Университета Райдера (США) Джон Сулер выдвинул концепцию «эффекта онлайн-растормаживания» (online disinhibition effect), чтобы описать влияние киберпространства на человека, при котором он действует свободнее, чем в реальном обществе. По его мнению, основу этого эффекта составляют: *диссоциативная анонимность* («ты меня не знаешь») – в условиях анонимности люди отделяют свои действия в киберпространстве от реального мира и личности, считая, что в такой ситуации можно не брать на себя ответственность; *невидимость* («ты меня не видишь») – позволяет избегать установления психологического контакта; *асинхронность* («увидимся позже») – возможность общения без необходимости немедленной реакции на слова или действия собеседника, что является важным дезингибирующим (растормаживающим) фактором; *солипсическая интроекция* («это всё в моей голове») – возникновение ощущения, что во время онлайн-общения все события происходят лишь в нашем личном воображении; *минимизация власти* («мы равны») – возникает из-за опосредованного восприятия признаков высокого социального статуса, а также возможности их игнорирования [19].

Виктимологические факторы. Согласно современным эмпирическим анализам, значительная часть киберинцидентов происходит с участием человеческого фактора. В частности, в отчете компании Verizon о расследовании утечек данных за 2025 год (Data Breach Investigations Report) отмечается, что примерно 60% нарушений связано с человеческим фактором (например, кибермошенничество, кража учетных данных или ошибочные действия) [20]. Европейские ученые М. Эванс, Л.А. Магларас, Ю. Хе и Х. Янике, исследуя вопросы информационной безопасности в государственном секторе, подчеркивают, что более двух третей (2/3) инцидентов в госорганизациях вызваны факторами, связанными с человеческой ошибкой, где человеческий фактор играет решающую роль [21]. Основная причина заключается в том, что пользователи недооценивают риски в Интернете, а преступники умело используют их доверчивость и незнание правил цифровой гигиены.

Низкий уровень киберграмотности населения и, в частности, халатное отношение пользователей к личной кибербезопасности, способствует глубокому укоренению современных киберугроз. Исследования показывают, что многие пользователи, обладая теоретическими знаниями о создании сложных паролей или использовании двухфакторной аутентификации, на практике не соблюдают эти протоколы безопасности. Это создает благоприятные условия для совершения киберпреступлений. По данным Международного

исследования компьютерной и информационной грамотности (ICILS), доля учащихся, не обладающих базовым уровнем цифровых навыков, составляет 51% в США и 43% в странах Евросоюза. Относительно положительный результат наблюдается в Южной Корее, где лишь 27% учащихся не имеют достаточных навыков [22]. Очевидно, что в нашей стране этот показатель значительно ниже, чем в вышеуказанных государствах.

Стоит отметить, что в настоящее время в науке уже сформировалось новое направление криминологии – кибервиктимология. Юрист Д.В. Жмуров определяет кибержертву как «лицо, группу или организацию, пострадавшую в результате преступных действий, совершенных в цифровой среде» [23]. С.А. Стяжкина разделяет жертв кибермошенничества на два основных типа: *жертвы технического воздействия* – в эту группу входит молодежь, активно использующая новые технологии и обладающая знаниями, но поверхностно относящаяся к вопросам компьютерной безопасности; их чрезмерная самоуверенность и потеря бдительности становятся причиной кибератак; *жертвы информационного воздействия* – к этой категории относятся чрезмерно доверчивые лица, легко поддающиеся психологическому влиянию и часто стремящиеся получить большую выгоду при минимальных затратах; они добровольно переводят деньги мошенникам или предоставляют свои конфиденциальные данные [1].

Технологические и инновационные факторы. Стремительный прогресс современных компьютерных технологий и ИИ способствует тому, что инструменты кибератак совершенствуются быстрее, чем системы защиты. Анонимность в сети и глобальный охват, в частности, маскировка IP-адресов и возможности дистанционного воздействия, открывают широкие пути для киберпреступности. Возможность полной анонимности пользователя устройства или сети в киберпространстве является не только технологическим, но и психологическим криминогенным фактором. Анонимность не только препятствует идентификации личности, но и позволяет предоставлять ложные сведения о себе, вступая в социальное взаимодействие под видом другого лица. В условиях анонимности любой человек чувствует возможность безнаказанного совершения негативных действий. Анонимность превращает киберпространство в «параллельный» мир по отношению к повседневной жизни и позволяет создавать новый образ, отличный от реального облика личности [24].

На сегодняшний день использование преступными группами возможностей искусственного интеллекта для создания вредоносных кодов и автоматизации фишинговых атак выводит угрозы информационной безопасности на качественнно новый уровень. Как отмечают ведущие американские эксперты и ученые в

области ИИ и кибербезопасности, такие как М. Брандидж, Ш. Авин, Дж. Кларк, Х. Тонер, П. Экерсли, в исследовании на тему «Злонамеренное использование искусственного интеллекта: прогнозирование, предотвращение и смягчение последствий», киберугрозы с участием ИИ характеризуются следующими особенностями: *во-первых*, эффективностью атак, то есть возможностью наносить больший ущерб при меньших затратах ресурсов за счет автоматизации; *во-вторых*, владением технологиями дезинформации и дипфейков (подмена или фальсификация человеческого облика или голоса с помощью ИИ) – в частности, способностью ИИ изменять видео до степени неразличимости от реальности для введения в заблуждение общественного мнения и обмана людей; *в-третьих*, сложностью контроля и мониторинга [25].

Экономические факторы. В современных научных статьях киберпреступность характеризуется как высокорентабельная экономическая сфера. Организация кибератаки требует минимальных вложений, в то время как потенциальная прибыль может исчисляться миллионами долларов. Авторитетные ученые в области информационной безопасности и основоположники научного направления «Экономика кибербезопасности» Росс Андерсон и Тайлер Мур в своих исследованиях отмечают, что сбои и проблемы в информационных системах возникают чаще из-за неверных экономических стимулов (мотивов), нежели из-за технических недостатков. Современные киберпреступления давно перешли от любительского уровня к специализированному разделению труда. В частности, появились такие «услуги», как написание вирусов под заказ, аренда ботнетов, продажа украденных данных и отмывание денег. Такая специализация повысила эффективность киберпреступности и снизила её издержки [26].

Более того, анонимность финансовых операций (транзакций) создает благоприятную среду для легализации доходов, полученных преступным путем, и присвоения средств посредством вымогательства.

Популяризация криптовалют в мировой экономике, их трансграничный характер и возможность в считанные секунды переводить миллионы долларов на другой конец света создают серьезные проблемы в борьбе с киберпреступностью. В частности, когда похищенные средства переходят в юрисдикцию другого государства, а также в случаях самой опасной формы киберпреступлений – «ransomware» (программ-вымогателей), требование хакеров оплачивать выкуп в криптовалютах типа Bitcoin делает практически невозможным замораживание или возврат этих средств правоохранительными органами.

Согласно анализу отчета по криптопреступности за 2025 год платформы Chainalysis, в последние

годы криптопреступность не только растет в объемах, но и становится более профессиональной и диверсифицированной. Если раньше криптопреступления ограничивались в основном кибератаками, то теперь они стали неотъемлемой частью организованной преступности и угроз национальной безопасности. Преступные группы всё более умело используют технологии блокчейн для отмывания денег, сочетая оффчейн- и ончейн-деятельность. Цифры показывают, что в 2024 году общая стоимость средств, полученных незаконными адресами, превысила 50 миллиардов долларов [27].

Правовые факторы. Правовые факторы совершения киберпреступлений проявляются в пробелах в законодательстве, нехватке норм международного права и сложностях установления уголовной ответственности. Одной из наиболее серьезных правовых проблем киберпреступности является вопрос юрисдикции, при котором преступник может находиться в одном государстве, сервер – в другом, а потерпевший – в третьем. Профессор Университета Монаша (Австралия) Дж. Клафф подчеркивает, что отсутствие территориальных границ в киберпространстве является основным препятствием для национальных правовых систем. Отсутствие двусторонних соглашений между многими государствами об экстрадиции киберпреступников или обмене цифровыми доказательствами создает в этой сфере определенные трудности [28].

Как справедливо отмечает международный эксперт в области кибербезопасности Штейн Шёльберг, киберпространство, являясь пятым общим пространством после суши, моря, воздуха и космоса, требует координации на международном уровне, сотрудничества и принятия особых правовых мер [29].

Еще одним юридическим фактором совершения киберпреступлений является недостаточное регулирование борьбы с ними на уровне международных актов. Хотя Будапештская конвенция (2001) является первым и наиболее важным международным документом в этой области, не все государства, в частности Россия и Китай, подписали её, что ослабляет глобальное сотрудничество [4]. Отсутствие единой глобальной системы борьбы с киберпреступностью создает для преступников своего рода «правовые убежища».

Очередной правовой фактор связан со сложностью сбора цифровых доказательств и процедурой их признания в суде, что требует от правоохранительных органов высокой технической квалификации.

Вышеизложенные тезисы, в частности специфические особенности киберпреступлений, факторы их возникновения и подпитки, а также обусловленная ими социальная опасность киберпреступности, диктуют необходимость реализации системных, последовательных и комплексных мер. *На наш взгляд, в*

данном процессе целесообразно уделить особое внимание следующим аспектам:

1. Переход к системам интеллектуальной защиты в обеспечении информационной безопасности. В условиях, когда для совершения и автоматизации кибератак используется искусственный интеллект, традиционные (статические) средства защиты теряют свою эффективность. В связи с этим необходимо внедрение систем «Интеллектуального мониторинга» (AI-driven security), способных прогнозировать кибератаки в режиме реального времени и адаптироваться к ним.

Согласно выводам исследования FATF (Группы разработки финансовых мер борьбы с отмыванием денег), одного лишь отслеживания блокчейна недостаточно; наиболее эффективным методом является установление комплексного мониторинга, объединяющего технические данные (IP, следы кошельков) и социальное поведение (принцип «Знай своего клиента» (KYC), экономическая логика) [30].

2. Создание общественного «Центра кибервиктимологии». Учитывая трансграничный и анонимный характер преступности в киберпространстве, целесообразно создать общественную структуру, основанную на социальном партнерстве правоохранительных органов и институтов гражданского общества. Рекомендуемые направления деятельности центра: *виктимологическая профилактика* – формирование системы киберпревенции через целевую пропаганду среди уязвимых слоев населения (молодежь, пожилые люди); *реабилитация и психологическая поддержка* – оказание специализированной помощи лицам, понесшим финансовый и моральный ущерб; *повышение иммунитета к кибермошенничеству* – формирование криминологической устойчивости к методам психологического манипулирования (социальной инженерии).

3. Совершенствование законодательства и международного сотрудничества. Актуальным является введение в Уголовный кодекс дефиниций «киберпреступление» и «виртуальная собственность». Необходимо признать совершение преступлений с использованием систем ИИ отягчающим обстоятельством и внедрить институт «технологической экспертизы» для разграничения алгоритмических ошибок ИИ и преступного умысла пользователя. Также важно сформировать единую практику, квалифицирующую технологическое хищение имущества как кражу, а манипуляцию волей через социальную инженерию – как мошенничество.

Целесообразно ускорить процесс присоединения Республики Узбекистан к Будапештской конвенции (2001), что позволит интегрироваться в сеть «24/7» для оперативного обмена цифровыми

доказательствами с зарубежными странами.

4. Повышение киберграмотности и укрепление цифровой гигиены. Рекомендуется внедрение комплексной стратегии обучения: *интеграция в систему непрерывного образования* – введение предмета «Основы кибербезопасности» в учебные программы с упором на «культуру цифрового поведения»; *сегментированный подход* – создание геймифицированного контента для подростков (борьба с кибербуллингом) и визуализированных пособий для старшего поколения по безопасному использованию цифровых финансовых услуг.

Заключение. Киберпреступления – это не только результат технических сбоев, но и сложный социально-правовой феномен. Реализация предложенных концептуальных мер позволит трансформировать стратегию кибербезопасности государства из стадии «защиты» в стадию «проактивной профилактики», формируя у общества устойчивый «цифровой иммунитет» к новым формам криминальной девиантности.

References:

1. Стяжкина С.А. Виктимологическая профилактика кибермошенничества // Вестник Удмуртского университета. Экономика и право. – 2022. – № 3. – С. 546-552.
2. Аккаева Х.А. Киберпреступления: криминологический анализ // Право и управление. – 2025. – № 1. – С. 317-322.
3. Критически рассмотрена деятельность органов правопорядка, определены новые задачи по обеспечению общественной безопасности // [Электронный ресурс] URL: https://president.uz/ru/lists/view/8882; Борьба с организованной преступностью и киберпреступностью будет усилена // [Электронный ресурс] URL: https://president.uz/ru/lists/view/9009 (дата обращения: 15.03.2026).
4. The Convention on Cybercrime (Budapest Convention, ETS No. 185) and its Protocols // [Электронный ресурс] – URL: https://www.coe.int/en/web/cybercrime/the-budapest-convention (дата обращения: 22.02.2026).
5. Самурханов М.С. Понятие и особенности киберпреступности // International Journal of Humanities and Natural Sciences. – 2020. – Т. 4–3, – №43. – С. 219-221.
6. Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: дис. ... канд. юрид. наук: 12.00.08. – Владивосток, – 2005. – С. 36.
7. Рассолов И.М. Информационное право. – М.: Юрайт, – 2011. – 44 с.
8. Кильметова Р.Р., Савлохов Р.Р., Пухаев Д.К., Икоев А.А., Хлоев А.Х. Современные виды мошенничества в сети интернет и пути их разрешения // Аграрное и земельное право. – 2025. – № 7. – С. 264–268.
9. Сергеева А.А., Гурев М.С., Кириллова Я.М. и др. Некоторые особенности противодействия мошенничеству, совершаемому с использованием электронных средств платежа, по законодательству России и Китая / Вопросы безопасности. – 2024. – № 1. – С.10.

10. Басханов А.М., Грицианова К.П. Кибербуллинг — новая угроза обществу // Евразийская адвокатура. – 2024. – № 5 (70). – С.124.
11. Phillips K., Davidson J.C., Farr R.R., Burkhardt C., Caneppele S., Aiken M.P. Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies // Forensic Sci. – 2022. – № 2, – pp.379–398.
12. Головко М.Н. Киберпреступность в зарубежных странах: виды и определения // Гуманитарные науки. Высшая школа. – 2025. – № 2, – С.47–50.
13. Ahmead M., El Sharif N., Abuiram I. Risky online behaviors and cybercrime awareness among undergraduate students at Al-Quds University: a cross-sectional study // Crime Science. – 2024. – №13. – Article 29.
14. Маслиенко М.А. Киберпреступность на современном этапе // Проблемы правоохранительной деятельности. – 2021. – №2. – С. 30.
15. Гомонов Н.Д. Интернет: анализ криминогенных факторов // Научный портал МВД России. – 2013. – № 4. – С. 34-38.
16. Лакомов А.С. Киберпреступность: современные тенденции // Академическая мысль. – 2019. – №2 (7). – С. 55.
17. Wandhöfer R. Top cyber threats and prevention trends in 2026 // [Электронный ресурс] URL: https://www.finextra.com/the-long-read/1507/top-cyber-threats-and-prevention-trends-in-2026 (дата обращения: 19.02.2026).
18. Transcript of the National Summit on Cyberethics // [Электронный ресурс] – URL: http://connect.marymount.edu/ethics/cyberethics/sessions/gensession3.PDF. – pp.23. (дата обращения: 19.02.2026).
19. John Suler. The Psychology of Cyberspace // [Электронный ресурс] – URL: http://users.rider.edu/~suler/psycyber/psycyber.html (дата обращения: 22.02.2026).
20. Verizon. 2025 Data Breach Investigations Report: Executive Summary. Verizon Business, 2025. // [Электронный ресурс] https://www.verizon.com/business/resources/reports/2025-dbir-executive-summary.pdf// (дата обращения: 20.02.2026).
21. Evans M., Maglaras L.A., He Y., Janicke H. Human behaviour as an aspect of cybersecurity assurance // Information & Computer Security. – 2019. – № 1 (27), – pp. 2–23.
22. European Commission. Lagging digital literacy among 14-year-olds across the EU, study finds [Электронный ресурс]. – URL: https://education.ec.europa.eu/news/lagging-digital-literacy-among-14-year-olds-across-the-eu-study-finds (дата обращения: 23.02.2026).
23. Жмуров Д.В. Индивидуальная виктимологическая профилактика киберпреступности // Сибирский юридический вестник. – 2023. – № 1. – С. 52-59.
24. Косенков А.Н., Черный Г.А. Общая характеристика психологии киберпреступника // Criminology Journal of Baikal National University of Economics and Law. – 2012. – № 3 (21). – С. 89.
25. Brundage M., Avin S., Clark J., Toner H., Eckersley P., Garfinkel B., Dafoe A., et al. The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. – Oxford: Future of Humanity Institute, 2018. – 101 p.

26. Moore T., Anderson R. Economics and Internet Security: a Survey of Recent Analytical, Empirical and Behavioral Research. – Cambridge: Harvard University, 2011. – 34 p.
27. Chainalysis. The 2025 Crypto Crime Report. – Chainalysis, 2025 // [Электронный ресурс] – URL: https://www.chainalysis.com (дата обращения: 22.02.2026).
28. Clough J. Principles of Cybercrime. – 2nd ed. – Cambridge: Cambridge University Press, 2015. – 30 p.
29. Stein Schjolberg. A cyberspace treaty – A United Nations convention or protocol on cybersecurity and cyber crime // [Электронный ресурс] – URL: http://cybercrimelaw.net/documents/UN_12th_Crime_ Congress.pdf (дата обращения: 22.02.2026).
30. Virtual Assets: Red Flag Indicators of Money Laundering and Terrorist Financing. – Paris: FATF, 2020. – 24 p.