Мақала туралы мәлімет / Содержание

«ЖАСТАР ЖӘНЕ ҒЫЛЫМ: БҮГІНІ МЕН БОЛАШАҒЫ» жас ғалымдардың халықаралық ғылыми-тәжірибелік конференция материалдар жинағы

Сборник материалов Международной научно-практической конференции молодых ученых «МОЛОДЕЖЬ И НАУКА: НАСТОЯЩЕЕ И БУДУЩЕЕ»

The collection of materials from the International Scientific and Practical Conference of Young Scientists «YOUTH AND SCIENCE: PRESENT AND FUTURE»

Жинақ	IV, Атырау, 8/04/2026, 2026 ж.
ISBN	978-601-262-638-4
Секция	СЕКЦИЯ IV. ЭКОНОМИКА ЖӘНЕ ҚҰҚЫҚ ҒЫЛЫМДАРЫ / ЭКОНОМИЧЕСКИЕ И ЮРИДИЧЕСКИЕ НАУКИ Секция IV.II. Цифрлық технологиялар жағдайындағы құқықтық жүйені дамыту және құқық қолдану тәжірибесі / Развитие правовой системы и практика правоприменения в условиях цифровых технологий
Жинақтағы рет нөмірі	№ 049
Мазмұндағы беті	232
Жарияланған беттері	232-237
Автор(лар)	Брюквин Мадиар Денисович
Мақала атауы	АКТУАЛЬНЫЕ ТЕНДЕНЦИИ КИБЕРПРЕСТУПНОСТИ В КАЗАХСТАНЕ И ПРОБЛЕМЫ РАСКРЫВАЕМОСТИ ЦИФРОВЫХ ПРЕСТУПЛЕНИЙ
Мазмұндағы жазылуы	Брюквин М.Д., Лукманова Н.А.АКТУАЛЬНЫЕ ТЕНДЕНЦИИ КИБЕРПРЕСТУПНОСТИ В КАЗАХСТАНЕ И ПРОБЛЕМЫ РАСКРЫВАЕМОСТИ ЦИФРОВЫХ ПРЕСТУПЛЕНИЙ

Ескерту: бет нөмірлері жинақтың соңындағы «МАЗМҰНЫ» бөліміндегі жарияланған беттерге сәйкес берілді.

УДК 343.97

«АКТУАЛЬНЫЕ ТЕНДЕНЦИИ КИБЕРПРЕСТУПНОСТИ В КАЗАХСТАНЕ И ПРОБЛЕМЫ РАСКРЫВАЕМОСТИ ЦИФРОВЫХ ПРЕСТУПЛЕНИЙ»

Брюквин Мадиар Денисович
channelmellberg@gmail.com
Студент 3-го курса образовательной программы «Правоохранительная деятельность»
Атырауского Университета им. Х.Досмухамедова, Атырау, Казахстан.
Научный руководитель, м.ю.н, сеньор-лектор -Лукманова Н.А.

Актуальность данной темы обусловлена совокупностью социально-экономических, технологических, правовых и геополитических факторов, которые формируют новую среду общественных отношений и одновременно создают новые угрозы национальной безопасности. В условиях активной цифровой трансформации государства киберпространство стало самостоятельной сферой общественных отношений, требующей комплексного правового регулирования, институционального обеспечения и научного осмысления. Республика Казахстан на протяжении последних лет реализует стратегию цифровизации государственного управления, экономики и социальной сферы в рамках программы Цифровой Казахстан. Внедрение электронных государственных услуг, развитие электронного документооборота, цифровизация финансовых операций, интеграция информационных систем государственных органов существенно повысили эффективность управления, однако одновременно расширили пространство для совершения преступлений в цифровой среде. Увеличение числа пользователей сети Интернет, распространение мобильных устройств, развитие финтех-сервисов и дистанционного банковского обслуживания формируют уязвимости, которые активно используются злоумышленниками. Киберпреступность отличается высокой латентностью, транснациональным характером и технологической сложностью. В условиях Казахстана эти особенности приобретают дополнительное значение, поскольку государство является частью глобального цифрового пространства и активно интегрируется в международные экономические и информационные процессы. Трансграничный характер киберпреступлений затрудняет расследование, требует международного сотрудничества, унификации правовых подходов и совершенствования механизмов экстрадиции и правовой помощи. Нормативную основу противодействия киберпреступности формирует Уголовный кодекс Республики Казахстан, предусматривающий ответственность за неправомерный доступ к информации, создание и распространение вредоносных программ, нарушение правил эксплуатации информационных систем, мошенничество с использованием информационно-коммуникационных технологий и

иные деяния. [1] Однако динамика цифровых технологий опережает темпы обновления законодательства, что создает пробелы в правовом регулировании и требует научного анализа для выработки предложений по его совершенствованию. Особую актуальность приобретает проблема квалификации преступлений, совершаемых с использованием информационно-коммуникационных технологий. В правоприменительной практике нередко возникают сложности разграничения традиционных составов преступлений и их цифровых форм. Например, мошенничество в сфере электронной коммерции, фишинговые атаки, незаконное получение доступа к банковским счетам через вредоносные программы требуют детального анализа объективной и субъективной стороны состава преступления, установления способа совершения и оценки причиненного ущерба. Рост безналичных расчетов и активное использование электронных платежных систем усиливают риски финансовых киберпреступлений. Банковский сектор Казахстана активно внедряет цифровые сервисы, что повышает доступность финансовых услуг, но одновременно увеличивает вероятность несанкционированного доступа к персональным данным и денежным средствам граждан. Защита информации в этой сфере становится вопросом не только частной безопасности, но и устойчивости финансовой системы государства. Развитие электронного правительства и цифровых платформ приводит к накоплению значительных массивов информации о физических и юридических лицах. Утечка таких данных способна повлечь серьезные последствия — от финансовых потерь до подрыва доверия к государственным институтам. В этой связи особое значение имеет анализ механизмов правовой охраны информации и ответственности за ее незаконное распространение. Киберпреступность затрагивает не только экономическую сферу, но и политическую стабильность государства. Информационные атаки, распространение деструктивного контента, вмешательство в работу государственных информационных систем могут представлять угрозу национальной безопасности. В условиях геополитической напряженности защита киберпространства становится элементом оборонной политики и стратегической устойчивости. [2]

В Республике Казахстан наиболее распространённые виды киберпреступлений отражают глобальные тенденции, но имеют национальные особенности, связанные с уровнем цифровизации экономики, распространением электронных услуг и правоприменительной практикой. Среди них можно выделить несколько ключевых категорий. Мошенничество с использованием информационно-коммуникационных технологий. Этот вид преступлений занимает лидирующие позиции. Злоумышленники применяют фишинговые схемы, поддельные интернет-сайты, социальную инженерию, рассылки с целью получения доступа к банковским счетам, электронным кошелькам или персональным данным. Чаще всего жертвами становятся пользователи онлайн-банкинга, платформ электронных платежей и маркетплейсов. Суммы ущерба варьируются от небольших денежных переводов до крупных хищений через корпоративные и государственные системы. Несанкционированный доступ к информации и информационным системам. Этот вид преступлений включает взлом компьютерных систем, сетевых ресурсов, баз данных государственных органов и организаций. Злоумышленники используют уязвимости программного обеспечения, кражу паролей и технические средства обхода защиты. Такие действия могут привести к утечке персональных данных, нарушению функционирования информационных систем и причинению экономического или репутационного ущерба. Злоумышленники создают и распространяют программы, которые блокируют работу компьютеров, шифруют данные, похищают информацию или используют ресурсы жертв для атак на третьих лиц. В Казахстане фиксируются случаи заражения корпоративных и государственных сетей, что приводит к временной остановке деятельности организаций и финансовым потерям. Киберпреступления против интеллектуальной собственности. Этот вид включает незаконное копирование, распространение и продажу программного обеспечения, медиаконтента, баз данных и других цифровых активов. В условиях активного роста электронной коммерции и цифровых сервисов такие преступления приобретают экономический характер, нанося ущерб авторам и правообладателям. Преступления, связанные с онлайн-экстремизмом, пропагандой

запрещенного контента и кибербуллингом. Особую опасность представляют случаи распространения экстремистских материалов через социальные сети и мессенджеры. Эти деяния привлекают внимание правоохранительных органов в контексте защиты общественной безопасности и несовершеннолетних. Финансовые киберпреступления с использованием криптовалют и цифровых платформ. С ростом популярности криптовалют и токенизированных активов участились случаи мошенничества в этой сфере, включая фальшивые ICO, взломы кошельков и схемы по переводу незаконно полученных средств. Киберпреступления против критической инфраструктуры. Несмотря на меньшую частоту, эти действия представляют стратегическую опасность. Они могут включать атаки на энергетические системы, транспортные и телекоммуникационные сети, государственные информационные системы, приводя к дестабилизации или нарушению функционирования жизненно важных объектов. Эти категории часто пересекаются, а один инцидент может включать несколько видов преступлений одновременно. Важной особенностью является транснациональный характер: злоумышленники могут находиться за пределами страны, что осложняет расследование и квалификацию преступлений. [3]

В Казахстане статистика киберугроз показывает значительное увеличение числа зарегистрированных инцидентов и преступлений в сфере информационной безопасности. По информации Комитета правовой статистики и специальных учётов Генеральной прокуратуры РК, за десять месяцев 2025 года в Едином реестре досудебных расследований зарегистрировано 201 преступление, связанное с несанкционированным доступом к данным, распространением вредоносных программ и другими нарушениями в сфере информатизации — это почти вдвое больше, чем за тот же период прошлого года.

Цифровые доказательства являются ключевым элементом расследования киберпреступлений, поскольку большая часть деяний совершается в информационной среде, где материальные следы практически отсутствуют. Порядок получения, фиксации и оценки таких доказательств требует строгого соблюдения процессуальных норм и технических стандартов, чтобы сохранить их достоверность, допустимость и юридическую силу. [4]

Ключевые проблемы квалификации киберпреступлений связаны с особенностями цифровой среды, сложностью технических действий и трансграничным характером деяний. Одна из основных проблем — разграничение смежных составов. Многие киберпреступления имеют аналогичные признаки с традиционными преступлениями: например, кибермошенничество может быть похоже на классическое мошенничество, хищение информации через электронные сети на преступления против собственности, а атаки на информационные системы могут сочетаться с уничтожением данных или нарушением работы объектов. Ошибки в разграничении приводят к неверной квалификации, недоказанности умысла или смягчению наказания. Проблема установления субъективной стороны преступления также является ключевой. Умысел, мотив и цель могут быть скрыты за использованием анонимных сетей, прокси, VPN, автоматизированных программ и чужих аккаунтов. Особая сложность связана с квалификацией трансграничных преступлений. Действия субъекта могут выполняться через иностранные серверы, международные платформы или криптовалютные сервисы, что усложняет применение национальных статей УК РК, установление юрисдикции и допустимости доказательств. Часто необходимо учитывать законодательство нескольких стран, что увеличивает риск ошибок в квалификации. Сложности возникают и при оценке цифровых доказательств. Неправильная фиксация, недостаточная экспертиза или технические ошибки могут привести к признанию доказательств недопустимыми. Это влияет на квалификацию и правовую оценку деяния, поскольку без доказательств невозможно установить субъект, объект, умысел и последствия преступления. Недостаточно развито законодательное регулирование новых технологий. Использование искусственного интеллекта, блокчейн-систем, автоматизированных атак и децентрализованных платформ создаёт ситуации, которые не всегда прямо подпадают под существующие статьи УК РК, что требует уточнения диспозиций или введения специальных норм. Ключевые проблемы квалификации заключаются в недостаточной интеграции

юридических и технических аспектов, ограниченной подготовке следователей и судей, сложности разграничения смежных составов, затруднённой установке субъективной стороны, особенностях трансграничных деяний и неопределённости законодательства относительно новых технологий. [5]

Основные трудности расследования киберпреступлений обусловлены особенностями цифровой среды, технической сложностью действий и трансграничным характером преступлений. Во-первых, это анонимность и скрытность действий преступников. Использование VPN, прокси-серверов, TOR-сетей, поддельных аккаунтов и псевдоанонимных криптовалют затрудняет установление личности субъекта и связь его действий с конкретным деянием. Преступники могут действовать дистанционно, через посредников, чужие устройства или автоматизированные программы, что усложняет сбор доказательств и установление умысла. Во-вторых, техническая сложность деяний требует привлечения специалистов по компьютерной криминалистике и применению современных методов экспертизы. Восстановление удалённых данных, анализ логов серверов, выявление вредоносного программного обеспечения и исследование сетевых соединений требуют высококвалифицированных кадров и специализированных инструментов. Недостаток таких ресурсов затрудняет проведение полноценного расследования. В-третьих, проблемы возникают при взаимодействии с банками, IT-компаниями и международными организациями. Запросы информации могут задерживаться из-за внутренних регламентов, необходимости соблюдения правил защиты персональных данных или различий в законодательстве других стран. Это особенно критично для трансграничных преступлений, где доказательства находятся на иностранных серверах или обрабатываются через зарубежные сервисы. В-четвёртых, трудности связаны с квалификацией преступлений и разграничением смежных составов.Ошибки в квалификации могут привести к недоказанности умысла или снижению меры ответственности. В-пятых, значительную сложность создаёт сохранение и фиксация цифровых доказательств. Данные легко поддаются удалению, модификации или фальсификации, а недостаточно стандартизированные процедуры изъятия и хранения увеличивают риск недопустимости доказательств в суде. Наконец, ускоренное развитие технологий создаёт трудности адаптации законодательных и процессуальных норм. Появление новых средств совершения преступлений, автоматизированных атак, блокчейн-технологий и искусственного интеллекта требует постоянного обновления методик расследования и подготовки специалистов. Основные трудности расследования киберпреступлений включают анонимность и скрытность действий преступников, техническую сложность, проблемы взаимодействия с банками и IT-компаниями, трудности квалификации и разграничения составов, сохранение цифровых доказательств и необходимость постоянного обновления знаний и методик. [6]

Предложения по совершенствованию законодательства и правоприменительной практики в сфере киберпреступлений основаны на выявленных проблемах квалификации, расследования и доказательной базы, а также на международном опыте и современных тенденциях цифровой преступности. Во-первых, предлагается уточнение диспозиций действующих статей УК РК и введение специальных норм, адаптированных к особенностям киберпреступлений. Это касается незаконного доступа к информации, кибермошенничества, распространения вредоносного программного обеспечения, атак на критически важные объекты и использования современных технологий, включая искусственный интеллект, блокчейн и децентрализованные платформы. Уточнённые формулировки позволят разграничивать смежные составы, учитывать дистанционный и трансграничный характер действий, а также более точно определять субъективную сторону преступления. Во-вторых, рекомендуется развитие положений о цифровых доказательствах, стандартизация процедур их изъятия, фиксации и оценки. Законодательство должно закреплять требования к сохранению целостности данных, применению компьютерно-технических экспертиз, а также регламентировать порядок взаимодействия следственных органов с банками, IT-компаниями и международными организациями. Это снизит риск недопустимости доказательств и повысит

качество расследования. В-третьих, обосновано усиление норм международного сотрудничества и интеграция положений о трансграничных преступлениях. Законодательство должно чётко определять юрисдикцию, правила обмена доказательствами, процедуры взаимной правовой помощи и экстрадиции, а также обеспечивать согласование действий с иностранными правоохранительными органами. Это позволит более эффективно расследовать международные киберпреступления и предотвращать правовую неопределённость. В-четвёртых, предлагается усиление организационных и технических мер: создание централизованных координационных структур, развитие методик совместной работы следствия и компаний, внедрение современных инструментов анализа цифровых следов и защиты критически важных объектов. Эти меры позволят ускорить расследование, минимизировать ошибки квалификации и повысить общественную безопасность. В-пятых, обосновано повышение квалификации следователей и судей через специализированные учебные программы, практическую подготовку на кейсах и лабораторных исследованиях, регулярное обновление знаний в области цифровых технологий, экспертиз и международного опыта. Методические рекомендации и стандарты расследования обеспечат единообразие подходов и правильную оценку цифровых доказательств. В совокупности эти предложения направлены на создание комплексной системы: адаптированного законодательства, стандартизированных процедур, профессионально подготовленных кадров, современных технических средств и эффективного международного сотрудничества. Их реализация позволит повысить эффективность расследования киберпреступлений, точность квалификации, качество доказательственной базы и защиту интересов государства, граждан и юридических лиц. [7]

Перспективы противодействия киберпреступности в Республике Казахстан зависят от комплексного подхода, который объединяет законодательные, организационные, технические и кадровые меры. Динамичное развитие цифровых технологий и рост трансграничных преступлений требует постоянного обновления уголовно-правовой регламентации, внедрения специальных норм и уточнения диспозиций УК РК, а также адаптации к новым способам совершения преступлений, включая автоматизированные атаки, использование искусственного интеллекта и криптовалют. Организационные меры, включая создание централизованных координационных структур, стандартизацию процедур изъятия и оценки цифровых доказательств, взаимодействие с банками, IT-компаниями и международными партнёрами, позволяют повысить оперативность расследований и качество правоприменения. Усиление технических мер, развитие компьютерно-технической экспертизы и внедрение современных инструментов анализа цифровых следов создают условия для своевременного выявления и пресечения преступлений. Ключевым элементом перспектив является подготовка кадров: повышение квалификации , специализированные программы обучения, практическая работа с кейсами и лабораторные исследования обеспечивают компетентное использование законодательства, правильную квалификацию преступлений и оценку доказательств. Международное сотрудничество и применение лучших практик других стран позволяют преодолевать трансграничные барьеры и повышать эффективность расследований. В совокупности перспективы противодействия киберпреступности в Казахстане связаны с интеграцией законодательства, технических и организационных мер, профессиональной подготовки кадров и международного взаимодействия. Реализация этих направлений позволит создать систему, способную эффективно выявлять, расследовать и предотвращать киберпреступления, минимизировать правовую неопределённость и защитить интересы государства, граждан и юридических лиц в условиях цифровой трансформации экономики и общества.

Список использованной литературы:

1.Уголовный кодекс Республики Казахстан от 3 июля 2014 г. № 226-V Режим доступа: https://adilet.zan.kz/rus/docs/K1400000226 – Дата обращения: 31.03.2026.

2.Борьба с киберпреступностью Режим доступа: https://liter.kz/borbu-s-kiberprestupnostiu-usilivaiut-v-kazakhstane-1752057922/ – Дата обращения: 31.03.2026.

3.Доля кибермошенничества в структуре преступности достигла значительного уровня // Kazakhstan Today. – Режим доступа: https://www.kt.kz/rus/crime/dolya_kibermoshennichestva_v_strukture_prestupnosti_dostigla_1377982994.html – Дата обращения: 31.03.2026.

4.Конвенция о киберпреступности (Будапештская конвенция) Режим доступа: https://www.coe.int/en/web/octopus/-/kazakhstan – Дата обращения: 31.03.2026.

5. Less than half of criminal cases on cybercrimes reached court in Kazakhstan // KazTAG. – Режим доступа: https://kaztag.kz/en/news/less-than-half-of-criminal-cases-on-cybercrimes-in-2024-reached-court-in-kazakhstan – Дата обращения: 31.03.2026.

6.Преступления в сфере информационных технологий Wikipedia. – Режим доступа: https://ru.wikipedia.org/wiki/… – Дата обращения: 31.03.2026.

7.Применение положений Будапештской конвенции в расследовании онлайн-мошенничества в Казахстан – Режим доступа: https://law-vestnik.buketov.edu.kz/law/article/download/751/570/2181 – Дата обращения: 31.03.2026.