ВЕСТНИК ИНСТИТУТА ЗАКОНОДАТЕЛЬСТВА
И ПРАВОВОЙ ИНФОРМАЦИИ
РЕСПУБЛИКИ КАЗАХСТАН
НАУЧНО-ПРАВОВОЙ ЖУРНАЛ
ISSN 2788-5283
eISSN 2788-5291
ТОМ 81, НОМЕР 1(2026), 277-291

**УДК 343.985.7;
004.05
ГРНТИ 10.77.01;
10.79.01
DOI 10.52026/2788-5291_2026_81_1_277
Научная статья**

© К.С. Лакбаев[1], Б.М. Нургалиев[2], А.Т. Садвакасова[3*], 2026
[1,2,3] Карагандинский университет Казпотребсоюза, Караганда, Казахстан
(e-mail: [1]k.lakbaev@mail.ru; [2]nbake@mail.ru; [3]adel_sadvakasova@mail.ru)

СОВРЕМЕННЫЕ ВЫЗОВЫ И ПРЕВЕНТИВНЫЕ МЕХАНИЗМЫ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

Аннотация. Статья посвящена анализу современного состояния и перспектив противодействия киберпреступности с акцентом на преступления, совершаемые в скрытых сегментах интернета (Darknet). Предметом исследования выступают организационно-правовые и технологические аспекты борьбы с высокотехнологичными преступлениями. Целью работы является формирование научно обоснованного подхода к разработке наступательной стратегии обеспечения цифровой безопасности. В исследовании использованы методы системного анализа, сравнительного правоведения, криминологической диагностики и контент-анализа эмпирических данных. Особое внимание уделено анализу инфраструктуры Darknet, включая особенности маршрутизации с использованием технологии TOR и способы сокрытия цифрового следа. Рассматриваются современные технологии деанонимизации участников, включая методы «honeypot», «moving target defense» и «two-sided deception». Приводятся примеры успешных операций по пресечению преступной активности в Darknet, в том числе операции «RapTor» и «Serengeti», с указанием конкретных результатов и изъятых цифровых доказательств.

Представленные в исследовании выводы акцентируют внимание на актуальности трансформации существующей парадигмы противодействия киберпреступности: от преимущественно реакционного подхода — к проактивной стратегии превенции. Такая стратегия требует комплексного применения интеллектуальных цифровых технологий, включая алгоритмы машинного обучения, методы обработки и интерпретации массивов неструктурированных данных, а также совершенствование оперативно-розыскных механизмов в условиях цифровой среды. В работе обоснована необходимость модернизации системы профессиональной подготовки специалистов в сфере кибербезопасности, уполномоченных на реализацию мер по выявлению, локализации и нейтрализации преступной деятельности в информационно-телекоммуникационном пространстве. Область применения результатов научной статьи включает совершенствование нормативно-правовой базы, разработку ведомственных методических рекомендаций и внедрение технологических решений в деятельность субъектов кибербезопасности. Авторами сделан обоснованный вывод о необходимости системного, междисциплинарного подхода к обеспечению цифровой безопасности в условиях стремительной трансформации преступных практик в сфере информационных технологий.

Ключевые слова: киберпреступность; Darknet; TOR; цифровая безопасность; деанонимизация; искусственный интеллект; информационные технологии; превенция; оперативно-розыскная деятельность; цифровое расследование.

Введение

В последние годы наблюдается устойчивая тенденция к выдвижению киберпреступлений на передовые позиции в структуре общей преступности как на национальном уровне, в частности в Республике Казахстан, так и в международной плоскости. На сегодняшний день общественное восприятие всё чаще сталкивается с фактами совершения уголовно наказуемых деяний с использованием цифровых технологий, в том числе таких традиционных форм, как мошенничество и кражи, остающиеся значимым сегментом совокупности уголовно наказуемых деяний. Наиболее типичной формой реализации подобной преступной активности являются схемы дистанционного введения в заблуждение посредством телефонной связи, а также неправомерные манипуляции, осуществляемые через соци-

* автор для корреспонденции. E-mail: adel_sadvakasova@mail.ru.

альные медиа-платформы и иные инструменты электронного взаимодействия.

В указанном контексте особую тревогу вызывает высокая степень латентности таких деяний, сопряжённая с их трансграничной природой, что в совокупности существенно повышает уровень их общественной опасности. Следует подчеркнуть, что киберпреступность в современном её проявлении уже не ограничивается экономически мотивированными деяниями вроде мошенничества и краж, но всё активнее проникает в иные сферы противоправной активности. В частности, речь идёт о бесконтактной торговле наркотическими средствами, их пропаганде, рекламировании, а также склонении к потреблению запрещённых веществ посредством цифровых платформ.

Наряду с этим, растущее распространение получают преступления, направленные на неправомерное завладение персональными данными граждан — с целью последующего вымогательства, шантажа и иных форм давления. Особую угрозу представляют и действия, подрывающие устойчивость функционирования жизненно важных информационных систем, включая банковские структуры, государственные регистры, транспортные и энергетические системы. Таким образом, киберпреступность трансформируется в многослойное социально опасное явление, подрывающее как правопорядок, так и национальную цифровую безопасность.

Сложившееся положение осложняется устойчивыми общественными представлениями, формирующими иллюзию безнаказанности киберпреступной деятельности, а также недостаточной эффективностью механизмов уголовного преследования лиц, причастных к совершению противоправных деяний в цифровой среде. Несмотря на наличие институционализированных структур, обеспечивающих информационную безопасность[1], потенциал правоохранительных органов по идентификации, документированию и привлечению к ответственности субъектов высокотехнологичных преступлений остаётся ограниченным, что способствует сохранению чувства неотвратимости наказания лишь в теории, но не в реальной практике.

Анализ существующей правоприменительной практики демонстрирует постепенное формирование и институционализацию методических подходов к противодействию преступлениям, совершаемым в информационно-коммуникационной среде. Указанные алгоритмы активно внедряются в оперативную деятельность как национальных правоохранительных органов, так и специализированных международных структур, охватывая как глобальный уровень, так и региональные юрисдикции отдельных государств.

Так, 26 ноября 2024 года Интерпол обнародовал информацию о реализации масштабной координированной операции под кодовым обозначением «Serengeti», охватившей территорию девятнадцати африканских стран. В ходе указанного мероприятия сотрудниками компетентных органов было произведено задержание свыше 1000 субъектов, подозреваемых в совершении деяний, нарушающих правопорядок в информационно-коммуникационной среде. Среди выявленных противоправных практик зафиксированы распространение программ-вымогателей (ransomware), компрометация служебной электронной корреспонденции (business email compromise), реализация схем цифрового вымогательства, а также различные формы сетевого мошенничества. Совокупный материальный ущерб, причинённый в результате преступной деятельности указанных лиц, предварительно оценён в 193 миллиона долларов США. Дополнительно в рамках данной операции было ликвидировано свыше 134 тысяч элементов вредоносной цифровой инфраструктуры, используемой в составе организованных преступных объединений[2].

В период с января по апрель 2025 года в рамках международной операции Operation Secure, проведённой с участием представителей силовых струк-

[1] Концепция кибербезопасности («Киберщит Казахстана»). Утверждена постановлением Правительства Республики Казахстан от 30 июня 2017 года №407 // URL: http://mdai.gov.kz/ru/pages/koncepciya-kiberbezopasnosti-kibershchit-kazahstana (дата обращения: 02.08.2025).

[2] Интерпол арестовал 3500 человек и $300 млн в 34 странах по делу о глобальной сети киберпреступников // URL: https://www.tadviser.ru/index.php (дата обращения: 02.08.2025).

тур из 26 стран совместно с Интерполом, были деактивированы свыше 20 000 IP-адресов и доменных имён, задействованных в распространении вредоносного программного обеспечения класса infostealer. Из оборота изъяты 41 сервер и более 100 гигабайт информации, связанной с преступной деятельностью, а также задержаны 32 лица, причастные к данным нарушениям. Дополнительно было направлено более 216 000 уведомлений потенциальным потерпевшим с рекомендациями по обеспечению информационной безопасности (включая смену паролей и блокировку доступа)[3].

В феврале 2025 года Интерпол при организационной поддержке AFRIPOL инициировал реализацию оперативного мероприятия Red Card в семи странах Африки — Бенине, Кот-д'Ивуаре, Нигерии, Руанде, Южно-Африканской Республике, Того и Замбии[4]. В результате координированных действий были задержаны 306 фигурантов, конфисковано 1842 технических устройства (мобильные телефоны, SIM-карты и прочее). Зафиксировано свыше 5000 пострадавших от преступных схем, включавших мошенничество с использованием мобильного банкинга, инвестиционных платформ и мессенджеров[5].

Несмотря на позитивные результаты указанных мероприятий, необходимо отметить, что эволюция форм и способов реализации противоправной активности в киберсреде требует постоянного обновления и совершенствования методического инструментария, применяемого правоохранительными органами.

Целью настоящего исследования является комплексный анализ современных вызовов противодействия киберпреступности в условиях цифровой трансформации с акцентом на преступную активность в анонимизированных сегментах сети Интернет (Darknet), а также обоснование перехода от преимущественно реактивной модели реагирования к проактивной, превентивной стратегии обеспечения цифровой безопасности. Для достижения поставленной цели, предполагается решить следующие задачи: проанализировать современные формы и тенденции киберпреступной деятельности, включая трансграничные и латентные преступления в цифровой среде; исследовать инфраструктурные и технологические особенности функционирования Darknet и сети TOR с точки зрения их использования в противоправных целях; обобщить практику международных и национальных операций по выявлению и пресечению киберпреступлений; проанализировать возможности применения современных технологических инструментов деанонимизации и активной киберзащиты (honeypot, moving target defense, two-sided deception); обосновать необходимость модернизации организационно-правовых и кадровых механизмов противодействия киберпреступности в условиях цифровизации.

Материалы и методы

Настоящее исследование основано на междисциплинарном подходе, сочетающем юридический, криминологический и информационно-аналитический инструментарий для комплексного анализа проблем выявления и противодействия киберпреступлениям. В эмпирическую основу исследования включены официальные отчёты и пресс-релизы международных организаций (Интерпол, Европол), данные KZ-CERT при АО «Государственная техническая служба», а также материалы открытых расследований, касающихся крупных инцидентов утечки данных и международных операций по нейтрализации транснациональной киберпрестности (операции Serengeti, Secure, Red Card и др.). Отдельное внимание было уделено статистическим данным по динамике киберинцидентов за 2023–2025 гг., как в глобальном масштабе, так и на уровне Республики Казахстан. Методологическую основу работы составили следующие научные подходы и методы: сравнительно-правовой метод,

[3] 20,000 malicious IPs and domains taken down in INTERPOL infostealer crackdown // URL: https://www.interpol.int/en/News-and-Events/News/2025/20-000-malicious-IPs-and-domains-taken-down-in-INTERPOL-infostealer-crackdown (date of reference: 03.08.2025).

[4] More than 300 arrests as African countries clamp down on cyber threats // URL: https://www.interpol.int/en/News-and-Events/News/2025/More-than-300-arrests-as-African-countries-clamp-down-on-cyber-threats (date of reference: 03.08.2025).

[5] Interpol Arrests Over 300 for Cyber Crimes in Africa // URL: https://westoahu.hawaii.edu/cyber/global-weekly-exec-summary/interpol-arrests-over-300-for-cyber-crimes-in-africa/ (date of reference: 03.08.2025).

контент-анализ открытых источников и специализированных публикаций, метод экспертной оценки, сетевой анализ (network forensics). Кроме того, в исследовании использовались результаты научных публикаций отечественных и зарубежных авторов, освещающих вопросы цифровой криминалистики, правового регулирования в условиях цифровизации, а также прикладных технологий противодействия злоумышленникам в киберсреде.

Обсуждение и результаты

Фундаментальной предпосылкой значительного числа киберпреступных деяний выступает относительно несложный доступ злоумышленников к персонализированной информации, позволяющий выстраивать доверительные коммуникации с предполагаемыми потерпевшими посредством использования методов социальной инженерии. Особую обеспокоенность вызывает тот факт, что подобные уязвимые сведения становятся общедоступными не только по причине утечек слабо защищённых баз данных, но и в результате неосознанного разглашения гражданами своих анкетных личных данных и сведений о себе посредством их размещения в открытых сегментах информационно-коммуникационного пространства — включая социальные медиа, цифровые платформы, а также при прохождении процедур авторизации и идентификации на различных интернет-сервисах.

В качестве подтверждения данной тенденции можно привести инцидент, имевший место в июне 2025 года, когда представители ТОО «ЦАРКА» (Центр анализа и расследования кибератак) официально подтвердили факт масштабной компрометации конфиденциальной информации, в результате чего в открытом доступе оказался архив, содержащий персональные данные порядка 16,3 миллиона граждан Республики Казахстан. Согласно официальной информации, в утекшем массиве содержались индивидуальные идентификационные номера (ИИН), фамилии, имена, отчества, даты рождения, адреса проживания, контактные номера телефонов, а также сведения медицинского характера, включая актуализированные записи за 2023–2024 годы[6].

Подобные инциденты, сопряжённые с нарушением принципов обработки и хранения персональных данных, создают благоприятную среду для реализации широкого спектра преступлений в киберпространстве, начиная от мошенничества и вымогательства, заканчивая фишингом, компрометацией электронных почтовых ящиков и незаконным получением доступа к банковским или иным защищённым сервисам. Выявленные факторы указывают на необходимость системного подхода к формированию политики в сфере защиты персональных данных, усиления цифровой гигиены пользователей, а также совершенствования механизмов оперативного реагирования на инциденты информационной безопасности.

Детализированное изучение указанных криминальных феноменов позволяет констатировать, что действующая модель противодействия киберпреступлениям в значительной степени носит односторонний и преимущественно реактивный характер. Существующая архитектура обеспечения информационной безопасности демонстрирует превалирование оборонительной тактики, при которой государственные институты преимущественно фиксируют и устраняют последствия уже совершённых нарушений, нежели осуществляют упреждающее воздействие на потенциальные угрозы.

Анализ экспертных оценок свидетельствует о доминировании в данном противостоянии концепции поэтапного реагирования, в рамках которой каждый инцидент влечёт за собой последующее закрытие обнаруженного уязвимого элемента системы. Так, в случае выявления хакером определённой лазейки, соответствующие службы спустя некоторое время разрабатывают и внедряют защитные механизмы, ликвидирующие выявленный риск[7].

[6] В июне 2025 года TSARKA подтвердил, что в Сеть утек архив с персональными данными ~16,3 млн жителей Казахстана, содержащий ИИН, ФИО, даты рождения, адреса, номера телефонов и медицинские данные — включая актуальные данные за 2023–2024 гг // URL: https://rus.baq.kz/utechka-goda-v-set-popali-personalnye-dannye-pochti-vsego-naseleniya-kazahstana_300015921/ (дата обращения: 03.08.2025).

[7] Honeypot: приманка для злоумышленника // URL: http://www.compdoc.ru/secur/internet/honeypot/ (дата обращения: 03.08.2025).

В условиях стремительного развития технологий киберпреступники оперативно осваивают новые уязвимости, сохраняя инициативу благодаря гибкости и технической оснащённости, что создаёт стратегический дисбаланс, при котором существующих мер недостаточно. Для эффективной киберзащиты требуется переход к проактивной модели, включающей превентивные стратегии, интеллектуальный анализ угроз и прогнозирование атак с целью их нейтрализации до реализации.

Для демонстрации уровня киберпреступности в Казахстане, целесообразным видится привести данные статистики по Республике Казахстан: в 2020 году уголовных правонарушений, предусмотренных главой 7 УК РК (Уголовные правонарушения в сфере информатизации и связи) было зарегистрировано 62, в 2021 – 74, в 2022 – 80, в 2023 – 78, в 2024 – 130 (Рис.1).

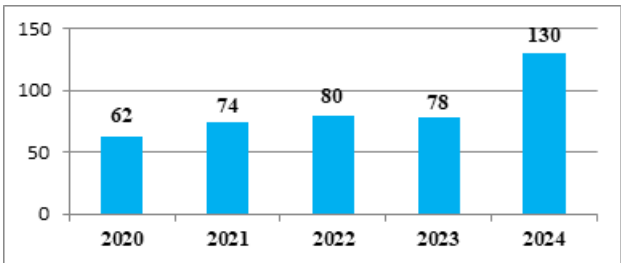

Рисунок 1. Регистрация фактов

По интернет-мошенничествам, в 2020 году было зарегистрировано 15 058 фактов, в 2021 году – 23 351, в 2022 году – 22 898, в 2023 году – 23 800, в 2024 году – 21 387 (Рис.2).

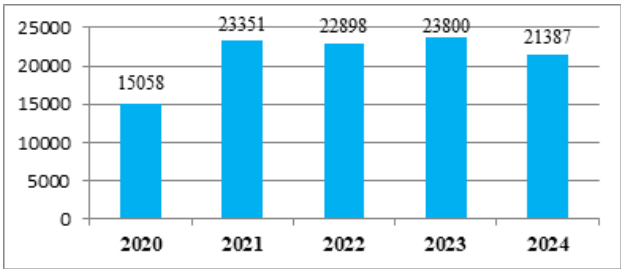

Рисунок 2. Регистрация фактов интернет-мошенничеств в период с 2020 по 2024 гг.

Правовой анализ показывает, что уголовно-правовое противодействие киберпреступности в Республике Казахстан опирается, прежде всего, на нормы, систематизированные в главе 7 УК РК («уголовные правонарушения в сфере информатизации и связи»), динамика регистрации которых в 2020–2024 гг. в статье используется как индикатор актуализации соответствующего массива посягательств. Одновременно содержание исследуемых угроз выходит за рамки «узкой» киберкриминализации: в цифровой среде воспроизводятся и трансформируются традиционные составы (в частности, интернет-мошенничество), а также формируются высокорисковые практики, связанные с незаконным оборотом запрещённых веществ и иными формами противоправной деятельности, что требует согласованного применения как специальных, так и общих уголовно-правовых запретов.

С учётом приведённых в работе примеров утечек персональных данных и их криминогенного эффекта, значимым элементом правового механизма выступает сопряжение уголовно-правовых норм с отраслевым регулированием информационных отношений и требований к защите данных. В исследовании демонстрируется, что компрометация массивов персональной информации и уязвимость цифровых сервисов создают предпосылки для последующих преступлений (вымогательство, фишинг, несанкционированный доступ), вследствие чего нормативная охрана должна рассматриваться не только как реакция на уже совершённое деяние, но и как режим предупреждения рисков — через требования к обработке/хранению данных и устойчивости информационных систем, включая критически значимые сегменты (банковские, государственные и др.).

Особую специфику правоприменения формирует преступность в Darknet: высокая анонимность TOR и затруднённость установления связи «лицо — действие» повышают значение процессуальных и оперативно-розыскных инструментов, обеспечивающих выявление, документирование и последующую проверку цифровых следов. Описанные в статье подходы (работа через технические узлы, мониторинг, внедрение и контрольные мероприятия, фиксация трафика и цифровых артефактов) показывают, что результативность достигается при сочетании традиционных полицейских методов и специализи-

рованных технологий; отсюда следует вывод о необходимости постоянного обновления ведомственных алгоритмов и методического инструментария применения таких мер в рамках действующего законодательства РК.

Для трансформации существующей модели противодействия киберугрозам необходим проактивный подход, основанный на раннем выявлении аномальной активности в сети. Одним из эффективных инструментов является технология Honeypot — имитированный объект, целенаправленно подвергающийся атаке. С его помощью фиксируются действия злоумышленников, анализируются их методы, формируются поведенческие шаблоны и выявляются новые векторы атак. Такая стратегия обеспечивает получение ценной информации о тактике хакеров и способствует формированию адаптивных механизмов информационной безопасности [1].

Кроме того, в арсенале активной киберзащиты представлены иные технологически продвинутые подходы. Одним из них является метод Moving Target Defense (MTD), суть которого заключается в постоянной модификации параметров информационной инфраструктуры — включая IP-адресацию, портовые настройки, версии операционных систем и иные конфигурации. Такая изменчивость препятствует точной идентификации целевых объектов злоумышленником, тем самым снижая вероятность успешной атаки и затрудняя проведение разведывательных операций [2].

Другой высокоэффективный метод — это технология Decoy-machines, реализуемая в рамках концепции двухсторонней обманной стратегии (two-sided deception). Она представляет собой усовершенствованную форму активной цифровой обороны, основанную на целенаправленном искажении восприятия атакующим стороной архитектуры защищаемой системы. В отличие от классических honeypot-механизмов, фокусирующихся на симуляции ограниченного числа сервисов, данный подход предполагает развертывание виртуализированных или аппаратных ловушек, которые не только маскируются под реальные компоненты инфраструктуры, но и искажают реакцию основной системы, создавая иллюзию согласованного взаимодействия.

Decoy-machine представляет собой автономный сетевой элемент — физический или виртуальный, внедрённый в ИТ-инфраструктуру с целью перехвата, документирования и последующего анализа вредоносной активности. Такая система обеспечивает не только сбор технических характеристик атаки, но и способствует выявлению тактик, техник и процедур (TTP) злоумышленников [3]. Применение двустороннего обмана позволяет существенно повысить эффективность аналитических механизмов, а также внедрить проактивные меры реагирования, направленные на упреждение угроз в условиях эволюционирующих киберрисков.

Таким образом, на начальном этапе необходимо систематизировать цифровые ресурсы, наиболее подверженные преступному вмешательству. Далее следует внедрить технологические решения, мониторить киберугрозы и выявлять уязвимости. На основе анализа формируется дифференцированная защита и алгоритм идентификации правонарушителей. Особую опасность представляют анонимные сегменты сети, включая Darknet, где высокая адаптивность киберпреступников и невозможность обнаружения традиционными средствами создают благоприятную среду для анонимных противоправных действий. Использование таких технологий может быть направлено как на реализацию легитимных прав – в том числе защиту конфиденциальности частной жизни и тайны переписки,– так и на осуществление противоправной либо запрещённой законом деятельности [4, с. 104].

По различным оценкам, доля Darknet в совокупной структуре Интернета составляет от 0,1 до 1 % [5,с.11;6;7]. Однако уровень его вовлечённости в преступную активность крайне высок. К приоритетным видам противоправной активности, реализуемой в анонимных сегментах цифрового пространства, относятся: незаконный оборот материалов порнографического характера, распространение наркотических веществ, совершение преступлений в сфере эконо-

мики, неправомерное получение конфиденциальной информации, дистрибуция экстремистского контента и пропаганда террористической идеологии, нелегальная торговля оружием, изготовление и сбыт поддельных документов и денежных знаков, а также иные деяния, предусмотренные уголовным законодательством [8, с. 99].

Доступ к скрытым ресурсам осуществляется посредством специализированного программного инструментария — маршрутизатора TOR (The Onion Router), функционирующего на основе технологии многоуровневого шифрования и последовательной ретрансляции данных с целью обеспечения полной анонимности участников сетевого взаимодействия [9, с. 85]. Передаваемая информация упаковывается в несколько уровней криптографической защиты, при этом активируются множественные промежуточные узлы-ретрансляторы [4, с. 104]. На стадии инициации передачи маршрутизатор осуществляет случайную генерацию цепочки из указанных узлов, формируя зашифрованный пакет и определяя для каждого из них адрес следующего элемента маршрута посредством использования алгоритма симметричного шифрования.

Уровень обеспечения анонимности пользователей в сегменте Darknet характеризуется как крайне высокий. Его архитектура изначально ориентирована на создание условий, при которых установление устойчивой корреляции между инициатором противоправной деятельности и её исполнителем становится предельно затруднённым, что существенно осложняет процедуру доказывания их взаимосвязи. В условиях отсутствия таких доказательств эффективность следственных действий резко снижается, а само уголовное преследование зачастую оказывается неэффективным.

В связи с этим ранее в экспертной среде доминировала точка зрения, согласно которой инфраструктура Darknet и технология маршрутизации TOR обеспечивают устойчивую защиту от выявления и контроля со стороны компетентных органов [10;11;12]. Однако с развитием криминалистических методов и расширением технических возможностей государственных структур стали разрабатываться и внедряться инструменты, направленные на деанонимизацию субъектов, действующих в анонимизированных сетях, и последующее их привлечение к юридической ответственности.

Например, Операция «RapTor» (май 2025), проведённая США при участии Европола и правоохранительных органов 10 стран, стала крупнейшим международным мероприятием по борьбе с наркоторговлей в Darknet. Арестовано 270 подозреваемых, изъято свыше 2 тонн наркотиков (включая 144 кг фентанила), 180 единиц оружия и более $200 млн. Операция выявила механизмы функционирования преступных платформ и подтвердила эффективность международного взаимодействия в деанонимизации и нейтрализации преступных сетей Darknet[8].

Постепенно учатся выявлять подобные преступления и в Казахстане. Так, в 2020 году крупнейшим примером выявления преступной деятельности через теневой интернет в Казахстане является случай, когда сотрудники спецслужб обнаружили подпольную нарколабораторию в г.Алматы, где синтетические вещества производились и распространялись через Darknet с расчётом в биткоинах. Ущерб оценён почти в 4 млн $, задержано 2 подозреваемых[9].

В 2024 году, в г.Костанай был задержан гражданин, организовавший мошеннические схемы через Darknet и Telegram, по отношению к гражданам иностранных государств. Он заработал значительные суммы, используя нелегальную торговлю личными данными и фальшивыми услугами[10].

Также, в апреле 2024 года, согласно данным Агентства финансового мониторинга Республики Казахстан, при мониторинге Telegram и Darknet были выявлены три крупных маркет-

[8] Law Enforcement Seize Record Amounts of Illegal Drugs, Firearms, and Drug Trafficking Proceeds in International Operation Against Darknet Trafficking of Fentanyl and Opioids; 270 Arrested Across Four Continents // URL: https://www.justice.gov/opa/pr/law-enforcement-seize-record-amounts-illegal-drugs-firearms-and-drug-trafficking-proceeds (date of reference: 03.08.2025).

[9] Спецслужбы нашли крупнейшую в истории Казахстана нарколабораторию // URL: https://www.bfm.ru/news/450254 (дата обращения: 03.08.2025).

[10] Хакер из Костаная заработал миллионы в DarkNet и Telegram // URL: https://tengrinews.kz/kazakhstan_news/haker-iz-kostanaya-zarabotal-millionyi-v-darknet-i-telegram-550292/ (дата обращения: 03.08.2025).

плейса, через которые осуществлялась продажа наркотиков. На площадках было зарегистрировано около 35 000 пользователей, а потенциальных клиентов — около 10 000. Оборот достиг порядка 3 млрд тенге. Выявлено более 80 активных Telegram-каналов, они функционировали как витрина Darknet-рынка[11].

Анализ практики раскрытия киберпреступлений демонстрирует интеграцию цифровых и традиционных полицейских методов. В частности, правоохранительные органы Новой Зеландии идентифицировали преступников через отслеживание почтовых отправлений — уязвимого звена Darknet-сделок. Отметим, что, несмотря на использование TOR и криптомессенджеров, доставка нередко осуществляется по реальным адресам. Элементы полицейской деятельности в различных странах включают внедрение под прикрытием, анализ изъятой информации, отслеживание финансовых потоков, в том числе криптовалют[12], а также деанонимизацию посредством выявления слабых мест в инфраструктуре сети анонимного доступа[13,14,15].

Важным является тот факт, что в сети TOR пользователи могут задействовать собственные вычислительные ресурсы для создания узлов (Node-серверов), выполняющих функции ретрансляции трафика. Наибольший интерес для целей выявления преступной активности представляют выходные узлы (exit nodes), поскольку они обеспечивают финальную стадию дешифровки трафика. Через такие точки возможен сбор информации о посещённых ресурсах, в том числе через заголовок HTTP-запроса, содержащий URL-источник. Существуют пассивные и активные модели мониторинга: первая предполагает анализ трафика через собственный узел, вторая – проведение MITM-атак с внедрением контролируемого сервера[16]. Суть атаки типа «Man-in-the-Middle» (MITM) заключается в перехвате и ретрансляции сетевого трафика через промежуточный узел, контролируемый злоумышленником, что позволяет осуществлять несанкционированный доступ к конфиденциальной информации, передаваемой пользователем, включая аутентификационные данные, такие как логины, пароли, персональные идентификационные номера и иные чувствительные сведения[17].

По нашему мнению, результативность описанных выше подходов может быть существенно усилена при интеграции с современными цифровыми технологиями, включая анализ больших данных (Big Data) и алгоритмы искусственного интеллекта (ИИ). Данные инструменты обладают значительным потенциалом в обработке и интерпретации массивов информации, поступающей в процессе противодействия преступной активности в киберпространстве. В этой связи, согласно экспертным оценкам, соотношение между оперативно-розыскной деятельностью и применением информационно-аналитических систем в борьбе с преступностью в сети Darknet составляет приблизительно 70% к 30% соответственно. Основной акцент в выявлении и нейтрализации преступных групп ложится на сотрудников оперативных подразделений. Несмотря на технологическую сложность среды, Darknet не исключает возможности сбора доказательственной информации. После того как зашифрованный трафик достигает конечного устройства правонарушителя, он обретает материальную форму, что позволяет его использовать в качестве вещественного доказательства, вне зависимости от методов шифрования. При этом возможно фиксировать сам факт передачи данных и применение сетей анонимного доступа, включая TOR.

Важно отметить, что конфиденци-

[11] Telegram и Darknet проверили на продажу наркотиков — АФМ // URL: https://cmn.kz/telegram-i-darknet-proverili-na-prodazhu-narkotikov-afm/ (дата обращения: 03.08.2025).

[12] Операция «Титан»: как полиция деанонимизировала покупателей наркотиков в Даркнете по всему миру // URL: http://www.furfur.me/furfur/changes/ changes/219311-hyperion (дата обращения: 04.08.2025).

[13] Операция Onymous // URL: https://ru.wikipedia.org/wiki/Operation_Onymous (дата обращения: 04.08.2025).

[14] Борьба с черными рынками интернета больше не обречена на провал // URL: https://vz.ru/society/2017/5/10/867799.html (дата обращения: 04.08.2025).

[15] Анализ сетевого трафика на сервере при помощи tshark // URL: https://blog.selectel.ru/analiz-setevogo-trafika-na-servere-pri-pomoshhi-tshark/ (дата обращения: 04.08.2025).

[16] Снифаем выходную ноду Tor'а и анализируем получившийся контент. Система мониторинга onion-доменов // URL: https://habr.com/ru/company/xakep/blog/244485/ (дата обращения: 03.08.2025).

[17] MITM-атака (атака «человек посередине») // URL: https://encyclopedia.kaspersky.ru/glossary/man-in-the-middle-attack/ (дата обращения: 04.08.2025).

альный характер оперативных мероприятий в киберпространстве играет ключевую роль при осуществлении доступа к закрытым сегментам сети Darknet. Значительная часть ресурсов этой анонимной сети функционирует на основе инвайт-систем – допуска к платформе только по специальному приглашению от уже зарегистрированных и проверенных пользователей. Для получения доступа к подобным ресурсам возможно использование внедрённых агентов или доверенных лиц, обладающих активной учетной записью, с целью входа под их идентификаторами.

Альтернативный путь – оперативное внедрение представителя правоохранительных органов в состав постоянных участников сайта с последующим получением статуса пользователя и осуществлением контрольной закупки. На этапе анализа маршрутов трафика по модели «от заказчика» или «от клиента» возможно использование данных интернет-провайдеров о соединении с входным узлом сети TOR. Путём соотнесения времени подключения к сети и совершения противоправного действия может быть сформирована причинно-следственная связь, указывающая на конкретное лицо. В большинстве случаев речь идёт о косвенных доказательствах, требующих комплексной оценки в совокупности с другими материалами уголовного дела.

Эффективность данной тактики возрастает при наличии предварительно идентифицированного подозреваемого. В таком случае устанавливается процессуальное наблюдение, в том числе контроль за почтовыми отправлениями, телеграфными сообщениями и иными видами коммуникации. Особое внимание уделяется мониторингу доставки объектов, заказанных предполагаемым правонарушителем, с целью фиксации его связи с преступной деятельностью в анонимных цифровых сетях.

Таким образом, проведённое исследование позволило выявить ряд закономерностей и конкретных результатов, касающихся как характера современных киберпреступлений, так и эффективных методик их выявления и пресечения. Прежде всего, констатировано, что киберпреступность в Казахстане и за его пределами приобретает системный характер, выходя за рамки отдельных эпизодов мошенничества. К традиционным видам преступлений (кража, мошенничество) прибавляются противоправные действия, связанные с оборотом наркотиков, распространением вредоносного программного обеспечения, компрометацией персональных данных, а также вмешательством в критически важные инфраструктуры, включая государственные и банковские информационные системы.

В теоретическом плане исследование подтвердило ограниченность действующих подходов, преимущественно ориентированных на реактивные (оборонительные) меры. Современные угрозы требуют перехода к проактивной, наступательной модели противодействия, в рамках которой реализуются технологии раннего предупреждения и превентивной фиксации подозрительной активности. В этом контексте обоснована эффективность применения систем типа Honeypot, позволяющих моделировать поведение атакуемого узла, анализировать инструменты злоумышленника и выявлять уязвимости до начала атаки на реальные системы. Дополнительно рассмотрены альтернативные инструменты активной защиты, включая Moving Target Defense и двухстороннюю стратегию обмана (two-sided deception) с использованием Decoy-machines.

Наиболее труднодоступной сферой остаётся борьба с преступностью в Darknet, характеризующаяся высокой степенью анонимности. Тем не менее, выявлены технические и тактические приёмы, позволяющие деанонимизировать участников скрытых сетей. В частности, анализ exit-узлов TOR, использование MITM-атак и внедрение агентуры в закрытые сообщества доказали свою результативность.

Обобщая полученные результаты, можно утверждать, что эффективное противодействие киберпреступности требует системного подхода, включающего превентивную аналитику, оперативную работу, юридическую грамотность и использование современных информационных технологий. Только при объединении всех этих компонентов возможно существенное повышение результативности борьбы с

киберугрозами и защита цифрового пространства государства.

Заключение

В результате проведённого исследования установлено, что киберпреступность в Республике Казахстан и в международном масштабе демонстрирует устойчивую тенденцию к усложнению и расширению предметной области: наряду с традиционными посягательствами (кражи и мошенничество) возрастают риски, связанные с оборотом наркотиков через цифровые платформы, распространением вредоносного ПО, компрометацией персональных данных и попытками воздействия на критически важные информационные системы. При этом латентность и трансграничный характер таких деяний объективно ограничивают эффективность «постфактум»-реагирования и усиливают потребность в методиках раннего выявления угроз и профилактического воздействия.

В исследовании конкретизировано, что действующая модель противодействия киберпреступлениям в значительной степени сохраняет преимущественно реактивный характер: меры концентрируются на устранении последствий и закрытии уже выявленных уязвимостей, тогда как технологическая динамика позволяет злоумышленникам быстро находить новые векторы атак. В этой связи обоснована необходимость трансформации парадигмы противодействия – от оборонительной тактики к проактивной, наступательной стратегии цифровой безопасности, основанной на упреждающей аналитике и ранней фиксации подозрительной активности в сети.

Отдельно показано, что наибольшие трудности для выявления и доказывания создаёт преступная активность в анонимизированных сегментах сети (Darknet), где технологии маршрутизации TOR и механизмы сокрытия цифрового следа существенно осложняют установление корреляции между участниками и действиями, а значит — снижают результативность традиционных следственных и оперативных подходов при отсутствии специальных технических решений. Одновременно в работе подтверждается, что даже в такой среде возможно формирование доказательственной базы при применении комбинации цифровых и традиционных полицейских методов, а также при использовании инструментов мониторинга и деанонимизации.

С практической точки зрения в исследовании конкретно выделены технологические направления усиления превентивного потенциала: применение систем класса Honeypot для моделирования атак и фиксации действий злоумышленников, использование подхода Moving Target Defense для снижения предсказуемости инфраструктуры и затруднения разведки атакующего, а также развитие двухсторонних обманных стратегий (two-sided deception) через Decoy-machines для перехвата и документирования вредоносной активности и выявления TTP. Данные инструменты рассматриваются не как разрозненные меры, а как элементы единой активной киберзащиты, работающей на опережение и поддерживающей аналитическую составляющую противодействия.

Ключевым организационно-кадровым результатом исследования является вывод о необходимости междисциплинарной подготовки специалистов, уполномоченных выявлять, локализовать и нейтрализовать киберпреступную деятельность: требуются компетенции одновременно в сфере юриспруденции и информационных технологий. Указано, что существующие модели профессиональной подготовки не в полной мере ориентированы на такую интеграцию, что затрудняет укомплектование специализированных подразделений. В связи с этим обоснована потребность в модернизации организационной структуры служб, реализующих функции кибербезопасности, с повышением их функциональной мобильности и внедрением современных цифровых аналитических инструментов.

Так, качественный рост эффективности противодействия киберпреступности возможен при одновременном устранении выявленных проблемных зон: усилении превентивной аналитики и активной киберзащиты, обновлении организационно-правового и методического инструментария, развитии кадрового потенциала и техническом переоснащении

профильных подразделений средствами мониторинга, анализа и идентификации цифровых следов правонарушений. Именно совокупность указанных мер, рассмотренных в работе, формирует основу для укрепления защищённости цифрового пространства и повышения результативности деятельности субъектов кибербезопасности.

Список литературы:

1. Jawale S.K. Intrusion Detection System using Virtual Honeypots. International Journal of Engineering Research and Applications - August 2022. P. 275-279. Available from: https://www.researchgate.net/publication/362910791_Intrusion_Detection_System_using_Virtual_Honeypots (date of reference: 02.08.2025).

2. Zhang L., Vrizlynn L. Three Decades of Deception Techniques in Active Cyber Defense - Retrospect and Outlook // Computers & Security. Available from: https://arxiv.org/abs/2104.03594 (date of reference: 02.08.2025).

3. Aggarwal P., Du Y., Singh K., Gonzalez C. Decoys in Cybersecurity: An Exploratory Study to Test the Effectiveness of 2-sided Deception // Computers & Security. Available from: https://arxiv.org/abs/2108.11037 (date of reference: 03.08.2025).

4. Смушкин А.Б. Криминалистические аспекты исследования даркнета в целях расследования преступлений // Актуальные проблемы российского права. 2022. №17. С. 102-111.

5. Васильев А., Ибрагимов Ж., Васильева О. Даркнет как ускользающая сфера правового регулирования // Юрислингвистика. 2019. № 12. С. 10-12.

6. Dockrill P. Only a Small Fraction of The Dark Web Is Being Used For Hidden Activity, Study Finds // ScienceAlert (Tech. Mag). 2020. Available from: https://www.sciencealert.com/only-a-small-fraction-of-the-dark-web-is-being-used-for-hidden-activity-study-finds (date of reference: 03.08.2025).

7. Avarikioti G., Brunner R., Kiayias A., Wattenhofer R., Zindros D. Structure and Content of the Visible Darknet // ArXiv, November. 2018. Available from: https://doi.org/10.48550/arXiv.1811.01348 (date of reference: 03.08.2025).

8. Бондаренко Ю.А., Кизилов Г.М. Проблемы выявления и использования следов преступлений, оставляемых в сети Darknet // Гуманитарные, социально-экономические и общественные науки. 2019. №5. С. 97-101.

9. Лакбаев К., Волчецкая Т., Нургалиев Б. Способы выявления и противодействия совершению киберпреступлений // Вестник КЭУ. 2025. №1(76). С. 82-88.

10. Karunanayake I., Ahmed N., Malaney R., Islam R., Jha S. De-anonymisation attacks on Tor: A Survey// IEEE Communications Surveys & Tutorials. 2021. Available from: https://www.researchgate.net/publication/352938766_De-anonymisation_attacks_on_Tor_A_Survey (date of reference: 03.08.2025).

11. Saleem J., Islam R., Kabir M.A. The Anonymity of the Dark Web: A Survey// IEEE Access. 2022. № 10. P. 33633–33657.

12. Jardine E., Lindner A.M., Owenson G. The Dark Web Dilemma: Tor, Anonymity and Online Policing//CIGI Paper. 2015. Available from: https://www.researchgate.net/publication/282612470_The_Dark_Web_Dilemma_Tor_Anonymity_and_Online_Policing (date of reference: 03.08.2025).

© К.С. Лакбаев[1], Б.М. Нургалиев[2], А.Т. Садвакасова[3], 2026
[1,2,3] Қазтұтынуодағы Қарағанды университеті, Қарағанды, Қазақстан
(e-mail: [1]k.lakbaev@mail.ru; [2]nbake@mail.ru; [3]adel_sadvakasova@mail.ru)

ЦИФРЛЫҚ ТРАНСФОРМАЦИЯ ЖАҒДАЙЫНДА КИБЕРҚЫЛМЫСҚА ҚАРСЫ ІС-ҚИМЫЛДЫҢ ҚАЗІРГІ ЗАМАНҒЫ СЫН-ТЕГЕУРІНДЕРІ МЕН АЛДЫН АЛУ ТЕТІКТЕРІ

Аннотация. Мақала Интернеттің жасырын сегменттерінде (Darknet) жасалған қылмыстарға баса назар аудара отырып, киберқылмысқа қарсы тұрудың қазіргі жағдайы мен перспективаларын талдауға арналған. Зерттеу тақырыбы жоғары технологиялық қылмыстармен күресудің ұйымдастырушылық-құқықтық және технологиялық аспектілері болып табылады. Жұмыстың мақсаты цифрлық қауіпсіздікті қамтамасыз етудің шабуыл стратегиясын әзірлеуге ғылыми негізделген тәсілді қалыптастыру болып табылады. Зерттеуде жүйелік талдау, салыстырмалы құқықтану, криминологиялық диагностика және эмпирикалық деректерді мазмұнды талдау әдістері қолданылды. Darknet инфрақұрылымын талдауға, соның ішінде Tor технологиясын қолдана отырып маршруттау ерекшеліктеріне және сандық іздерді жасыру тәсілдеріне ерекше назар аударылады. Қатысушыларды анонимизациялаудың заманауи технологиялары, соның ішінде «honeypot», «moving target Defence» және «two-sided deception» әдістері қарастырылуда. Darknet-тегі қылмыстық әрекеттердің, соның ішінде «RapTor» және «Serengeti» операцияларының нақты нәтижелері мен алынған цифрлық дәлелдерді көрсете отырып, сәтті тоқтату операцияларының мысалдары келтірілген.

Зерттеуде ұсынылған тұжырымдар киберқылмысқа қарсы іс — қимылдың қолданыстағы парадигмасын трансформациялаудың өзектілігіне назар аударады: негізінен реакциялық тәсілден-

алдын алудың белсенді стратегиясына. Мұндай стратегия машиналық оқыту алгоритмдерін, құрылымдалмаған деректер массивтерін өңдеу және түсіндіру әдістерін, сондай-ақ цифрлық орта жағдайында жедел-іздестіру тетіктерін жетілдіруді қоса алғанда, зияткерлік цифрлық технологияларды кешенді қолдануды талап етеді. Жұмыста ақпараттық-телекоммуникациялық кеңістіктегі қылмыстық қызметті анықтау, оқшаулау және бейтараптандыру жөніндегі шараларды іске асыруға уәкілеттік берілген киберқауіпсіздік саласындағы мамандарды кәсіптік даярлау жүйесін жаңғырту қажеттілігі негізделген. Ғылыми мақаланың нәтижелерін қолдану саласы нормативтік-құқықтық базаны жетілдіруді, ведомстволық әдістемелік ұсынымдарды әзірлеуді және киберқауіпсіздік субъектілерінің қызметіне технологиялық шешімдерді енгізуді қамтиды. Авторлар ақпараттық технологиялар саласындағы қылмыстық тәжірибелердің қарқынды трансформациясы жағдайында цифрлық қауіпсіздікті қамтамасыз етуге жүйелі, пәнаралық тәсілдің қажеттілігі туралы негізделген қорытынды жасады.

Түйінді сөздер: киберқылмыс; Darknet; TOR; цифрлық қауіпсіздік; деанонимизация; жасанды интеллект; ақпараттық технологиялар; алдын алу; жедел-іздестіру қызметі; цифрлық тергеу.

© K.S. Lakbayev[1], B.M. Nurgaliyev[2], A.T. Sadvakassova[3], 2026
[1,2,3] Karaganda University of Kazpotrebsoyuz, Karaganda, Kazakhstan
(e-mail: [1]k.lakbaev@mail.ru; [2]nbake@mail.ru; [3]adel_sadvakasova@mail.ru)

CONTEMPORARY CHALLENGES AND PREVENTIVE MECHANISMS FOR COUNTERING CYBERCRIME IN THE CONTEXT OF DIGITAL TRANSFORMATION

Abstract. The article is devoted to analyzing the current state and prospects of combating cybercrime, with a focus on crimes committed in hidden segments of the Internet (Darknet). The subject of the study is the organizational, legal, and technological aspects of combating high-tech crimes. The aim of the work is to develop a scientifically sound approach to the development of an offensive strategy for ensuring digital security. The study uses methods of system analysis, comparative law, criminological diagnostics, and content analysis of empirical data. Particular attention is paid to the analysis of the Darknet infrastructure, including the features of routing using TOR technology and methods of concealing digital traces. Modern technologies for de-anonymizing participants are considered, including the methods of «honeypot», «moving target defense», and «two-sided deception». Examples of successful operations to suppress criminal activity on the Darknet are given, including the RapTor and Serengeti operations, with specific results and seized digital evidence.

The conclusions presented in the study emphasize the relevance of transforming the existing paradigm of combating cybercrime: from a predominantly reactive approach to a proactive prevention strategy. Such a strategy requires the comprehensive application of intelligent digital technologies, including machine learning algorithms, methods for processing and interpreting unstructured data arrays, and the improvement of operational and investigative mechanisms in the digital environment. The paper substantiates the need to modernize the system of professional training for cybersecurity specialists authorized to implement measures to detect, localize, and neutralize criminal activity in the information and telecommunications space. The scope of application of the scientific article's findings includes improving the regulatory framework, developing departmental methodological recommendations, and introducing technological solutions into the activities of cybersecurity entities. The authors have made a well-founded conclusion about the need for a systematic, interdisciplinary approach to ensuring digital security in the context of the rapid transformation of criminal practices in the field of information technology.

Keywords: cybercrime; Darknet; TOR; digital security; de-anonymization; artificial intelligence; information technology; prevention; opera;ional-search activities; digital investigation.

References:

1. Jawale S.K. Intrusion Detection System using Virtual Honeypots. International Journal of Engineering Research and Applications - August 2022. P. 275-279. Available from: https://www.researchgate.net/publication/362910791_Intrusion_Detection_System_using_Virtual_Honeypots (date of reference: 02.08.2025).;

2. Techniques in Active Cyber Defense - Retrospect and Outlook // Computers & Security. Available from: https://arxiv.org/abs/2104.03594 (date of reference: 02.08.2025).

3. Aggarwal P., Du Y., Singh K., Gonzalez C. Decoys in Cybersecurity: An Exploratory Study to Test the Effectiveness of 2-sided Deception // Computers & Security. Available from: https://arxiv.org/abs/2108.11037 (date of reference: 03.08.2025).

4. Smushkin A.B. Kriminalisticheskie aspekty issledovanija darkneta v celyah rassledovaniya prestupleniy // Aktualnye problemy rossiyskogo prava. 2022. №17. S. 102-111.

5. Vasilyev A., Ibragimov Zh., Vasilyeva O. Darknet kak uskolzayushchaya sfera pravovogo regulirovaniya // Yurislingvistika. 2019. №12. S. 10-12.

6. Dockrill P. Only a Small Fraction of The Dark Web Is Being Used For Hidden Activity, Study Finds // ScienceAlert (Tech. Mag). 2020. Available from: https://www.sciencealert.com/only-a-small-fraction-of-the-dark-web-is-being-used-for-hidden-activity-study-finds (date of reference: 03.08.2025).

7. Avarikioti G., Brunner R., Kiayias A., Wattenhofer R., Zindros D. Structure and Content of the Visible Darknet // ArXiv, November. 2018. Available from: https://doi.org/10.48550/arXiv.1811.01348 (date of reference: 03.08.2025).
8. Bondarenko Yu.A., Kizilov G.M. Problemy vyyavleniya i ispolzovaniya sledov prestupleniy, ostavlyaemyh v seti Darknet // Gumanitarnye, sotsialno-ekonomicheskie i obshchestvennye nauki. 2019. №5. S. 97-101.
9. Lakbaev K., Volchetskaya T., Nurgaliev B. Sposoby vyyavleniya i protivodeistviya sovershenіyu kiberprestupleniy // Vestnik KJeU. 2025. №1(76). S. 82-88.
10. Karunanayake I., Ahmed N., Malaney R., Islam R., Jha S. De-anonymisation attacks on Tor: A Survey// IEEE Communications Surveys & Tutorials. 2021. Available from: https://www.researchgate.net/publication/352938766_De-anonymisation_attacks_on_Tor_A_Survey (date of reference: 03.08.2025).
11. Saleem J., Islam R., Kabir M.A. The Anonymity of the Dark Web: A Survey// IEEE Access. 2022. №10. R.33633–33657.
12. Jardine E., Lindner A.M., Owenson G. The Dark Web Dilemma: Tor, Anonymity and Online Policing// CIGI Paper. 2015. Available from: https://www.researchgate.net/publication/282612470_The_Dark_Web_Dilemma_Tor_Anonymity_and_Online_Policing (date of reference: 03.08.2025).

Авторлар туралы мәліметтер:

Лакбаев Канат Саметович – заң ғылымдарының докторы, профессор, Қазтұтынуодағы Қарағанды университеті экономикалық және құқықтық зерттеулер ғылыми-зерттеу институтының бас ғылыми қызметкер, Академическая көшесі, 9, 100000, Қарағанды, Қазақстан.
ORCID: https://orcid.org/0000-0003-1900-5250;
Scopus Author ID: 57200499422;
E-mail: k.lakbaev@mail.ru.
Нургалиев Бахыт Молдатьяевич – заң ғылымдарының докторы, профессор, Қазтұтынуодағы Қарағанды университеті экономикалық және құқықтық зерттеулер ғылыми-зерттеу институтының бас ғылыми қызметкер, Академическая көшесі, 9, 100000, Қарағанды, Қазақстан.
ORCID: https://orcid.org/0000-0002-3017-3610;
Scopus Author ID: 56275926800;
E-mail: nbake@mail.ru.
Садвакасова Адель Талғатқызы – хат хабарларға арналған автор, философия докторы (PhD), Қазтұтынуодағы Қарағанды университетінің экономикалық және құқықтық зерттеулер ғылыми-зерттеу институтының аға ғылыми қызметкер, Академическая көшесі, 9, 100000, Қарағанды, Қазақстан.
ORCID: https://orcid.org/0000-0001-5959-3718;
Scopus Author ID: 59668017300;
E-mail: adel_sadvakasova@mail.ru.

Алғыс. Авторлар Қазақстан Республикасы Ғылым және жоғары білім министрлігінің Ғылым комитетіне қаржыландырғаны үшін және рецензенттерге сараптамалық пікірлері мен конструктивті тәсілдері үшін алғыс білдіреді.

Дәйексөз келтіру үшін. Лакбаев К.С., Нургалиев Б.М., Садвакасова А.Т. Цифрлық трансформация жағдайында киберқылмысқа қарсы іс-қимылдың қазіргі заманғы сын-тегеуріндері мен алдын алу тетіктері // Қазақстан Республикасының Заңнама және құқықтық ақпарат институтының Жаршысы. Ғылыми-құқықтық журнал. 2026;81(1): 277-291. DOI – https:// doi.org/10.52026/2788-5291_2026_81_1_277.

Авторлардың қосқан үлесі:

Лақбаев Қ.С. – зерттеудің әдіснамалық негізін әзірледі, оның ішінде пәнаралық тәсілді таңдауды, жүйелік, салыстырмалы-құқықтық және желілік талдау әдістерін қолдануды айқындады. Сонымен қатар, ол мақаланы дайындауға ғылыми жетекшілік етті.

Нұрғалиев Б.М. – «Кіріспе» бөлімін дайындады. «Талқылау және нәтижелер» бөлімінде қолданыстағы құқық қолдану практикасына талдау жүргізіп, халықаралық операциялардың материалдарын жинақтап, анонимді желілердегі қылмыстық қызметті деанонимизациялау және оны анықтаудың тактикалық тәсілдері мәселелері бойынша негізгі қорытындыларды тұжырымдады.

Садвакасова А.Т. – статистикалық деректерді, соның ішінде киберинциденттер мен дербес деректердің жария болуына қатысты мәліметтерді өңдеу және талдау жұмыстарын жүргізді. Сондай-ақ, библиографиялық тізімді рәсімдеп, транслитерация жасап, аңдатпаның және авторлар туралы мәліметтердің ағылшын тіліндегі нұсқасын дайындады. Бұдан бөлек, цифрлық қорғау тетіктеріне, Honeypot, MTD технологияларына және екіжақты алдау стратегиясына арналған ғылыми жарияланымдарға контент-талдау жүргізді.

Авторлар бірлесіп «Талқылау және нәтижелер» бөлімінің қорытынды нұсқасын, сондай-ақ «Қорытынды» бөлімін тұжырымдады.

Осылайша, мақала құқықтық сараптаманы, талдамалық қызметті және техникалық сүйемелдеуді біріктірген үйлестірілген ғылыми жұмыстың нәтижесі болып табылады.

Мүдделер қақтығысы туралы ақпарат. Авторлар мүдделер қақтығысының жоқтығын туралы мәлімдейді.

Қаржыландыру көзі. Мақала Қазақстан Республикасы Ғылым және жоғары білім министрлігінің Ғылым комитеті (AP26198915 жобасының ЖСН) гранттық қаржыландыру шартын орындау шеңберінде дайындады.

Мақала редакцияға келіп түсті: 06.08.2025; рецензиялаудан кейін келіп түсті: 08.12.2025; басып шығаруға қабылданды: 31.03.2026.

Авторлар қолжазбаның соңғы нұсқасын оқып, мақұлдады.

Сведения об авторах:

Лакбаев Канат Саметович – доктор юридических наук, профессор, главный научный сотрудник Научно-исследовательского института экономических и правовых исследований Карагандинского университета Казпотребсоюза, улица Академическая, 9, 100000, Караганда, Казахстан.
ORCID: https://orcid.org/0000-0003-1900-5250;
Scopus Author ID: 57200499422;
E-mail: k.lakbaev@mail.ru.
Нургалиев Бахыт Молдатьяевич – доктор юридических наук, профессор, главный научный сотрудник Научно-исследовательского института экономических и правовых исследований Карагандинского университета Казпотребсоюза**,** улица Академическая, 9, 100000, Караганда, Казахстан.
ORCID: https://orcid.org/0000-0002-3017-3610;
Scopus Author ID: 56275926800;
E-mail: nbake@mail.ru.
Садвакасова Адель Талгатовна – автор для корреспонденции, доктор философии (PhD), старший научный сотрудник Научно-исследовательского института экономических и правовых исследований Карагандинского университета Казпотребсоюза, улица Академическая, 9, 100000, Караганда, Казахстан.
ORCID: https://orcid.org/0000-0001-5959-3718;
Scopus Author ID: 59668017300;
E-mail: adel_sadvakasova@mail.ru.

Благодарности. Авторы выражают благодарность Комитету науки Министерства науки и высшего образования Республики Казахстан за финансирование и рецензентам за экспертное мнение и конструктивный подход.

Для цитирования. Лакбаев К.С., Нургалиев Б.М., Садвакасова. А.Т. Современные вызовы и превентивные механизмы противодействия киберпреступности в условиях цифровой трансформации // Вестник Института законодательства и правовой информации Республики Казахстан. Научно-правовой журнал. 2026;81(1): 277-291. DOI – https:// doi.org/10.52026/2788-5291_2026_81_1_277.

Вклад авторов:
Лакбаев К.С. – разработал методологическую основу исследования, включая выбор междисциплинарного подхода, применение системного, сравнительно-правового и сетевого анализа. Осуществил научное руководство подготовкой статьи.
Нургалиев Б.М. – подготовил раздел «Введение». В разделе «Обсуждение и результаты» провел анализ существующей правоприменительной практики, обобщил материалы международных операций и сформулировал основные выводы по вопросам деанонимизации и тактических приёмов выявления преступной деятельности в анонимных сетях.
Садвакасова А.Т. – отвечала за обработку и анализ статистических данных, включая сведения по киберинцидентам и утечкам персональных данных, а также осуществила оформление библиографического списка, провела транслитерацию и подготовила англоязычную версию аннотации и информации об авторах. Кроме того, ею проведён контент-анализ научных публикаций, посвящённых цифровым механизмам защиты, технологиям Honeypot, MTD и двухсторонней обманной стратегии.
Авторами совместно сформулирован итоговый вариант раздела «Обсуждение и результаты», а также раздел «Заключение».
Таким образом, статья представляет собой результат скоординированной научной работы, объединяющей юридическую экспертизу, аналитическую деятельность и техническое сопровождение.

Информация о конфликте интересов. Авторы заявляют об отсутствии конфликта интересов.

Источник финансирования. Статья подготовлена в рамках выполнения договора на грантовое финансирование Комитетом науки Министерства науки и высшего образования Республики Казахстан (ИРН проекта AP26198915).

Статья поступила в редакцию: 06.08.2025; поступила после рецензирования: 08.12.2025; принята в печать: 31.03.2026.

Авторы прочитали и одобрили окончательный вариант рукописи.

Information about authors:

Lakbayev Kanat Sametovich – Doctor of Legal Sciences, Full Professor, Chief Researcher at the Scientific Research Institute of Economic and Legal Studies of the Karaganda University of Kazpotrebsoyuz, 9, Akademicheskaya Street, 100000, Karaganda, Kazakhstan.
ORCID: https://orcid.org/0000-0003-1900-5250;
Scopus Author ID: 57200499422;
E-mail: k.lakbaev@mail.ru.
Nurgaliyev Bakhyt Moldatyevich – Doctor of Legal Sciences, Full Professor, Chief Researcher at the Scientific Research Institute of Economic and Legal Studies of the Karaganda University of Kazpotrebsoyuz, 9, Akademicheskaya Street, 100000, Karaganda, Kazakhstan.
ORCID: https://orcid.org/0000-0002-3017-3610;
Scopus Author ID: 56275926800;
E-mail: nbake@mail.ru.
Sadvakassova Adel Talgatovna – corresponding author, Doctor of Philosophy (PhD), Senior Researcher at the Scientific Research Institute of Economic and Legal Studies of the Karaganda University of Kazpotrebsoyuz, 9, Akademicheskaya Street, 100000, Karaganda, Kazakhstan.
ORCID: https://orcid.org/0000-0001-5959-3718;
Scopus Author ID: 59668017300;
E-mail: adel_sadvakasova@mail.ru.

Acknowledgements. The authors would like to thank the Science Committee of the Ministry of Science and Higher Education of the Republic of Kazakhstan and the reviewers for their expert opinion and constructive approach.

For citation. Lakbayev K.S., Nurgaliyev B.M., Sadvakassova A.T. Contemporary challenges and preventive mechanisms for countering cybercrime in the context of digital transformation // Bulletin of Institute of Legislation and Legal Information of the Republic of Kazakhstan. Scientific and legal journal. 2026;81(1): 277-291. DOI https://doi.org/10.52026/27885291_2026_81_1_277.

Contribution of the authors:

Lakbaev K.S. – developed the methodological basis of the study, including the choice of an interdisciplinary approach, the use of systemic, comparative legal and network analysis. He also provided scientific guidance for the preparation of the article.

Nurgaliev B.M. – prepared the section **«**Introduction**»**. In the **«**Discussion and results**»** section, an analysis of existing law enforcement practice was conducted, materials from international operations were summarized, and the main conclusions on deanonymization and tactics for detecting criminal activity in anonymous networks were formulated.

Sadvakassova A.T. – was responsible for the processing and analysis of statistical data, including information on cyber incidents and personal data leaks, as well as carried out the design of the bibliographic list, carried out transliteration and prepared the English version of the abstract and information about the authors. In addition, she conducted a content analysis of scientific publications on digital protection mechanisms, Honeypot technologies, MTD and two-way deception strategy.

The authors jointly formulated the final version of the «Discussion and results» section, as well as the «Conclusion» section.

Thus, the article is the result of coordinated scientific work combining legal expertise, analytical activities and technical support.

Conflict of interest statement. The authors declares that there is no conflict of interest.

Funding. The article was prepared as part of the implementation of the grant financing agreement by the Science Committee of the Ministry of Science and Higher Education of the Republic of Kazakhstan (IRN AP26198915).

Received: 06.08.2025; revised: 08.12.2025; accepted for publication: 31.03.2026.

The authors has read and approved the final manuscript.