

ГРНТИ 10.77.01

УДК 343.2/.7

DOI: 10.54649/2077-9860-2026-1-66-74

Н.М. Батырбай^{1*}, Н.Д. Тлешалиев²

¹доктор PhD, заместитель декана высшей школы права «Адилет»
Каспийского общественного университета (г. Алматы, Казахстан)
e-mail: nurbol.ansar2019@gmail.com; ORCID ID: 0000-0002-9679-2262

²доктор PhD, руководитель управления профилактики коррупции
Департамента Агентства Республики Казахстан
по делам государственной службы по городу Алматы
(г. Алматы, Казахстан)

ORCID ID: 0000-0003-3871-866X; e-mail: ali_2301@mail.ru

БОРЬБА С ТРАНСНАЦИОНАЛЬНОЙ КИБЕРПРЕСТУПНОСТЬЮ СОТРУДНИКАМИ ПРАВООХРАНИТЕЛЬНЫХ И СПЕЦИАЛЬНЫХ ГОСУДАРСТВЕННЫХ ОРГАНОВ РЕСПУБЛИКИ КАЗАХСТАН

Аннотация

В статье рассматриваются актуальные вопросы борьбы с транснациональной киберпреступностью сотрудниками правоохранительных и специальных государственных органов Республики Казахстан. Проанализированы особенности и тенденции развития киберпреступности в условиях цифровизации и глобализации, а также выявлены ключевые проблемы, возникающие при её предупреждении, выявлении и расследовании. Особое внимание уделено анализу действующего законодательства Республики Казахстан и его соответствию международным стандартам в сфере противодействия киберугрозам. Рассмотрены вопросы межведомственного взаимодействия и международного сотрудничества, включая обмен информацией и участие в совместных операциях.

В ходе исследования использованы общенаучные и специальные методы, включая системный, сравнительно-правовой, статистический и формально-юридический анализ. На основе проведенного исследования сформулированы предложения, направленные на совершенствование нормативно-правовой базы, повышение эффективности деятельности правоохранительных и специальных органов, развитие цифровых технологий и укрепление международного взаимодействия.

Сделан вывод о необходимости комплексного подхода к противодействию транснациональной киберпреступности, включающего правовые, организационные и технологические меры. Так же в статье проведен анализ практики борьбы с транснациональной киберпреступностью, на основании которого выделены основные этапы, проблемы и предложены пути их разрешения. В связи с распространенностью и повышенной общественной опасностью киберугроз, данным вопросом озабочены многие отечественные и зарубежные исследователи.

Ключевые слова: транснациональная киберпреступность, противодействие преступности, предупреждение преступности, национальная безопасность, правоохранительные органы, преступность, меры.

*Автор-корреспондент, e-mail: nurbol.ansar2019@gmail.com

Введение

Использование сети Интернет растет экспоненциальными темпами: в настоящее время насчитывается более 3,8 млрд пользователей по всему миру, что составляет почти 47 % населения планеты. Согласно оценкам, пользователи проводят в социальных сетях около пяти лет своей жизни¹. Во многих странах резкий всплеск количества подключений к глобальной сети совпал по времени с экономическими и демографическими преобразованиями, ростом разрыва в доходах, сокращением расходов в частном секторе и снижением финансовой ликвидности. На общемировом уровне правоохранительные органы отмечают рост киберпреступности в связи с тем, что как частные лица, так и организованные преступные группы используют новые технологические возможности для совершения противоправных деяний, руководствуясь стремлением к извлечению прибыли и получению личной выгоды. Для совершения киберпреступлений более не требуется обладание сложными техническими навыками или знание специфических методов; достаточным условием является наличие умысла на совершение преступления.

Материалы и методы

В ходе исследования вопросов борьбы с транснациональной киберпреступностью, осуществляемого сотрудниками правоохранительных и специальных государственных органов Республики Казахстан, использовался комплекс общенаучных и частнонаучных методов познания. Материальную основу исследования составили: нормативные правовые акты Республики Казахстан, регулирующие вопросы противодействия киберпреступности; международные договоры и соглашения в сфере борьбы с транснациональной преступностью и киберугрозами; статистические данные правоохранительных органов Республики Казахстан; аналитические отчеты международных организаций; научные публикации отечественных и зарубежных авторов по проблемам кибербезопасности и транснациональной преступности.

Методологическую основу исследования составили следующие методы: диалектический метод – применялся для изучения закономерностей развития киберпреступности в условиях цифровизации общества и глобализации; системный анализ – использовался для рассмотрения деятельности правоохранительных и специальных органов как целостной системы противодействия транснациональной киберпреступности; сравнительно-правовой метод – позволил сопоставить национальное законодательство Республики Казахстан с международными стандартами и практикой зарубежных государств; формально-юридический метод – применялся при анализе действующих нормативных правовых актов; статистический метод – использовался для обработки и анализа данных о состоянии и динамике киберпреступности.

Результаты и обсуждение

Согласно сведениям компании Group-IB, за последнее десятилетие число и уровень сложности кибератак со стороны как прогосударственных хакерских групп, так и финансово мотивированных киберпреступников значительно возросли. Физические лица, коммерческие организации и государственные структуры более не могут быть уверены в безопасности киберпространства, а также в целостности и защищенности своих данных. Кибератаки осуществляются на международном уровне и характеризуются разнообразием направлений: проведение открытых военных операций с применением кибероружия; совершение кибератак, направленных на нарушение стабильности функционирования интернета на государственном уровне; наличие скрытых угроз со стороны проправительственных группировок; целенаправленные атаки на банки, страховые, консалтинговые компании, энергетические и ядерные корпорации².

Приведенные сведения о состоянии кибератак в глобальном масштабе обуславливают необходимость повышения потенциала страны, в частности правоохранительного блока, в части изучения и совершенствования практики расследования указанных деяний. Согласно Уголовному кодексу Республики Казахстан (далее – УК РК), транснациональная организованная группа определяется как организованная группа, преследующая цель совершения одного или нескольких уголовных правонарушений на территории двух или более государств либо одного государства

¹ Руководство Организации Объединенных Наций "Практическое руководство по порядку запроса электронных доказательств из других стран (для использования только правоохранительными и судебными органами)" январь 2020 г. URL: https://www.unodc.org/documents/organized-crime/GPTOC/GPTOC2/_ebook.pdf (дата обращения: 02.02.2026).

² Отчет Group-IB "HI-Tech crime trends 2019/2020. URL: <https://www.f6.ru/media-library/report/facct-hi-tech-crime-trends-2019-2020-trend-report-2019.pdf> (дата обращения: 03.02.2026).

при организации совершения деяния или руководстве его исполнением с территории другого государства, а равно при участии граждан другого государства¹.

По мнению В.А. Номоконова, «киберпреступность» представляет собой широкую область криминализации, включающую: деяния, направленные против конфиденциальности, целостности и доступности компьютерных данных или систем; деяния, предполагающие использование компьютера в целях извлечения личной или финансовой прибыли либо причинения личного или финансового вреда; а также деяния, связанные с содержанием компьютерных данных [1].

К правоохранительным органам относятся органы прокуратуры, внутренних дел, государственной противопожарной службы, антикоррупционная служба и служба экономических исследований, осуществляющие свою деятельность в соответствии с законодательными актами Республики Казахстан². Специальные государственные органы — это непосредственно подчиненные и подотчетные Президенту Республики Казахстан государственные органы, являющиеся составной частью сил обеспечения национальной безопасности, осуществляющие разведывательную и контрразведывательную деятельность, а также комплекс правовых, организационных, оперативно-розыскных и технических мер, направленных на обеспечение безопасности охраняемых лиц и объектов в целях предотвращения угроз национальной безопасности³.

Технические методы совершения киберпреступлений коренным образом трансформируют традиционные способы хищения денежных средств и иные деяния, совершаемые в целях получения финансовой выгоды в отношении организаций частного сектора. Расширение возможностей преступной деятельности, позволяющее не только совершать хищения в отношении предприятий, но и получать доступ к хранящимся сведениям личного и финансового характера посредством организации утечки данных, привело к существенному повышению уровня восприятия частным сектором рисков, связанных с киберпреступностью.

Международный аспект компьютерных преступлений, совершаемых с использованием отдельных или закрытых систем, получил признание в уголовном законодательстве уже в 1979 году. В рамках третьего Симпозиума Интерпола по вопросам международного мошенничества, состоявшегося 11-13 декабря 1979 года, была представлена презентация на тему компьютерного мошенничества, в которой подчеркивалось, что «компьютерные преступления носят международный характер, что связано с неуклонным развитием телефонной, спутниковой и иных видов связи между разными странами⁴.

Доказывание состоит в собирании, исследовании, оценке и использовании доказательств с целью установления обстоятельств, имеющих значение для законного, обоснованного и справедливого разрешения дела. Досудебное расследование осуществляется только по уголовным правонарушениям, по которым оно начато в порядке, предусмотренном главой 23 Уголовно-процессуального кодекса Республики Казахстан⁵.

Множество стран сообщают, что правоохранительным органам становится известно о деяниях в сфере киберпреступности из сообщений частных лиц или организаций, ставших жертвами таких деяний. В одном из глобальных обследований частного сектора указано, что 80 % частных лиц, ставших жертвами киберпреступлений, не сообщают об этом в правоохранительные органы. Редкое обращение потерпевших объясняется неосведомленностью о факте виктимизации, чувством стыда или неловкости, нежеланием быть вовлеченными в уголовный процесс (особенно если, по их мнению, им не причинен существенный вред), а в случае корпораций — опасениями репутационных рисков.

Указанные признаки латентности киберпреступлений в Республике Казахстан подтверждаются при сравнении сведений, представленных ГУ «Управление комитета по правовой статистике и специальным учетам Генеральной прокуратуры Республики Казахстан по городу Алматы» (далее — УКПСиСУ) и РГП «Государственная техническая служба» Комитета национальной безопасности Республики Казахстан (далее — ГТС КНБ РК). По данным УКПСиСУ, за период с 2015 по 2019 год в республике зарегистрировано 18 063 уголовных правонарушения в сфере информати-

¹ Уголовный кодекс Республики Казахстан от 3 июля 2014 года № 226-V. URL: <https://adilet.zan.kz/rus/docs/K1400000226> (дата обращения: 03.02.2026).

² Закон Республики Казахстан от 6 января 2011 года № 380-IV «О правоохранительной службе». URL: <https://adilet.zan.kz/rus/docs/Z1100000380> (дата обращения: 03.02.2026).

³ Закон Республики Казахстан от 13 февраля 2012 года № 552-IV «О специальных государственных органах Республики Казахстан». URL: <https://adilet.zan.kz/rus/docs/Z1200000552> (дата обращения: 03.02.2026).

⁴ Доклад Управления Организации Объединённых Наций по Наркотикам и Преступности «Всестороннее исследование проблемы киберпреступности» февраль 2013 г. URL: https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime_Study_Russian.pdf (дата обращения: 04.02.2026).

⁵ Уголовно-процессуальный кодекс Республики Казахстан от 4 июля 2014 года № 231-V. URL: <https://adilet.zan.kz/rus/docs/K1400000231> (дата обращения: 04.02.2026).

зации и связи, включая иные преступления, совершенные с использованием информационных технологий. В разбивке по годам ситуация выглядит следующим образом: в 2015 году зарегистрировано 663 преступления, в 2016 году – 1705, в 2017 году – 2818, в 2018 году – 5101, в 2019 году – 9164¹.

Согласно сведениям ГТС КНБ РК, в 2015 году в республике зарегистрировано 17 621 инцидент информационной безопасности, в 2016 году – 19 118, в 2017 году – 24 584, в 2018 году – 19 335, в 2019 году – 20 458. За 2019 год из 20 458 инцидентов информационной безопасности 17 496 совершены в отношении юридических лиц, а 2962 – в отношении государственных органов страны. Инциденты информационной безопасности в 2019 году распределены по следующим типам: ботнеты – 17520 (из них в отношении юридических лиц – 15627, государственных органов – 1 893); вредоносное программное обеспечение (вредоносный код на информационных ресурсах) – 409 (406 – юр. лица, 3 – гос. органы); несанкционированный доступ и модификация содержания интернет-ресурсов – 206 (201 и 5 соответственно); фишинг – 830 (828 и 2); DDoS-атаки – 185 (15 и 170); атаки на интернет-ресурсы – 18 (5 и 13); спам – 26 (4 и 2); отсутствие доступа к интернет-ресурсу – 949 (121 и 828); прочие – 314 (289 и 25)².

В 2015 году в УКПСиСУ зарегистрировано 663 уголовных дела, тогда как в ГТС зарегистрировано 17 621 инцидент информационной безопасности. Приведенные сведения свидетельствуют о том, что в 2015 году досудебные расследования проводились лишь по 3,8 % от всех инцидентов информационной безопасности. Аналогичная динамика по годам выглядит следующим образом: в 2016 году – 8,9 %, в 2017 году – 11,5 %, в 2018 году – 26,4 %, в 2019 году – 44,8 %. Таким образом, наблюдается низкий уровень регистрации киберпреступлений по сравнению с зарегистрированными ГТС инцидентами информационной безопасности. Если допустить, что часть инцидентов, фиксируемых ГТС, не регистрируется в Едином реестре досудебного расследования (что является реальной предпосылкой), то процент регистрации указанных фактов может оказаться существенно ниже. Низкий уровень регистрации киберпреступлений представляет собой лишь одну сторону проблемы. Вторая сторона, отражающая реальную эффективность работы правоохранительных органов, заключается в количестве дел, по которым виновные лица привлечены к уголовной ответственности.

Анализ соотношения количества уголовных дел, по которым виновные лица привлечены к уголовной ответственности, и количества зафиксированных инцидентов информационной безопасности показывает, что с 2015 года по 152 преступлениям виновные лица привлечены к уголовной ответственности, из них в суд направлено 132, прекращено по нереабилитирующим основаниям 20, что составляет 0,8 % от всех зарегистрированных инцидентов информационной безопасности за указанный период. Динамика по годам: в 2016 году – 78 дел (в суд – 38, прекращено – 40), что эквивалентно 0,4 %; в 2017 году – 207 дел (113 и 94 соответственно) – 1 %; в 2018 году – 979 дел (379 и 600) – 5 %; в 2019 году – 1 488 дел (567 и 921) – 7,3 %.

Приведенные данные свидетельствуют о недостаточном объеме следственно-оперативных мероприятий, направленных на раскрытие киберпреступлений. Одной из основных причин столь низких показателей раскрываемости и качества расследования является недостаточный уровень подготовки сотрудников правоохранительных органов при расследовании уголовных правонарушений в сфере информатизации и связи.

Указанная проблема носит не только национальный, но и общемировой характер. В настоящее время контроль над киберпреступностью представляет собой сложную задачу; вместе с тем необходимо наращивать практику расследования указанных преступлений. В этой связи органам уголовного преследования следует принять меры, направленные на тщательное изучение и совершенствование практики расследования киберпреступлений.

Повсеместное расширение подключения к глобальной сети создает серьезный риск роста уровня киберпреступности. Хотя доступ к надежным статистическим данным затруднен, исследования отмечают, что киберпреступность представляет собой нарастающий вызов, что подтверждается основополагающими криминологическими и социально-экономическими факторами. Например, одна из европейских стран отметила: «Опираясь на результаты исследований и статистические данные, предоставленные преимущественно частным сектором или научными кругами, сформировалось общее мнение о том, что количество киберпреступлений резко растет, в то время как возможности контролировать киберпреступность ограничены». Как отмечалось

¹ «Управление комитета по правовой статистике и специальным учетам Генеральной Прокуратуры РК по г.Алматы» за исх.№2-21603-20-00146 от 10.01.2020 г. URL: <https://qamqor.gov.kz/crimestat/indicators> (дата обращения: 03.02.2026).

² Ответ зарегистрированные инциденты информационной безопасности Службой реагирования на компьютерные инциденты KZ-CERTc 2015 по 2019 год за исх.№36/08-1/01-1-2057 от 11.10.2019 г. URL: <https://www.cert.gov.kz/> (дата обращения: 04.02.2026).

в Салвадорской декларации 2010 года о комплексных стратегиях для ответа на глобальные вызовы, принятой резолюцией 65/230 Генеральной Ассамблеи ООН, «развитие информационно-коммуникационных технологий и расширение масштабов использования Интернета создают новые возможности для преступников и способствуют росту преступности».

Подключение к глобальной сети должно рассматриваться как центральный элемент современной киберпреступности и, в особенности, киберпреступности будущего. По мере расширения киберпространства и IP-трафика, а также опережения объема трафика беспроводных устройств по сравнению с проводными и роста интернет-трафика, генерируемого некомпьютерными устройствами, становится затруднительным представить «компьютерное» преступление при отсутствии IP-подключения к глобальной сети. Особый персонализированный характер мобильных устройств и появление подключенных к интернет-протоколу бытовых приборов или личных вещей ведут к тому, что электронные данные и их передача могут генерироваться или становиться неотъемлемой частью практически каждого действия человека – как законного, так и незаконного.

Общая теория преступности, касающаяся снижения уровня самоконтроля и готовности принимать риск ради получения краткосрочной выгоды, также может быть применима к преступлениям, совершаемым при помощи или с использованием электронных средств связи и Интернета. Кроме того, если лица находят в глобальной сети информацию о киберпреступниках, ориентируясь на них как на модель поведения, или общаются в сети со сверстниками, совершающими киберпреступления, вероятность совершения ими киберпреступления возрастает. Данная теория социального научения может оказаться особенно актуальной в случае киберпреступлений, поскольку преступникам нередко необходимо изучить специфические компьютерные приемы и процессы. Теория социального научения и общая теория преступности взаимно дополняют друг друга: лица, характеризующиеся пониженным уровнем самоконтроля, стремятся найти подобных себе лиц и объединяются в виртуальном пространстве так же, как и в реальном мире. В киберпространстве данный процесс может происходить значительно быстрее и охватывать более обширные географические регионы.

Подключение к глобальной сети и обмен опытом с себе подобными являются основными факторами, способствующими совершению киберпреступлений организованными преступными группами. Одним из примеров являются онлайн-форумы «кардинга» (мошенничества, связанного с хищением данных кредитных карт), которые используются для обмена украденной информацией. Такие форумы нередко зарождаются в форме «роевой» структуры при отсутствии иерархической цепи управления, когда преступники находят друг друга и «встречаются» в глобальной сети для обмена знаниями и предоставления преступных услуг.

Согласно сведениям Group-IB, в 2019 году «кардинг» стал наиболее быстрорастущим сегментом в области угроз клиентам банков. Рынок сбора данных банковских карт продолжает расти на протяжении нескольких лет. Его можно условно разделить на два сегмента: текстовые данные (номер, дата истечения срока действия, имя держателя, адрес, CVV-код) и дампы (содержимое магнитной полосы карт). За 2019 год количество скомпрометированных карт выросло с 27,1 до 43,8 млн по сравнению с 2018 годом. Согласно данным Group-IB, в 2019 году средняя цена на текстовые данные выросла с 9 до 14 долларов США, при этом средняя цена дампа снизилась с 33 до 22 долларов США. Общее количество скомпрометированных карт по текстовым данным в 2019 году составило 12 540 190 шт. (размер рынка – 179 159 552 долларов США), по дампам – 31 213 941 шт. (размер рынка – 700 520 520 долларов США).

Социально-экономические факторы влияют на рост киберпреступности как в развитых, так и в развивающихся странах. Согласно сведениям ГТС КНБ РК, в Республике Казахстан зафиксирована активность хакеров, осуществляющих атаки и попытки несанкционированного доступа к компьютерным данным или системам (возможно, в целях промышленного шпионажа), в том числе в отношении государственных органов. Указанные хакеры после кибератак оставляют свои псевдонимы или характерный «почерк». На основании этих сведений можно предположить, что некоторые хакеры являются гражданами Республики Казахстан. Приведенные данные свидетельствуют о наличии и даже о процветании хакерской активности в стране. Учитывая стремительное развитие интернета, было бы необоснованным полагать, что в стране отсутствует значительное количество лиц, занимающихся или потенциально готовых совершать киберпреступления. Немаловажную роль также играет слабая информационная защищенность или ее отсутствие у физических и юридических лиц, что дополнительно привлекает иностранных киберпреступников, рассматривающих их как легкую добычу.

В этой связи необходимо повышение потенциала правоохранительных органов страны по взаимодействию с иностранными и отечественными поставщиками услуг в целях выявления и

раскрытия киберпреступлений, совершаемых на территории нашей страны и за ее пределами. Согласно оценкам Организации Объединенных Наций, свыше 80 % киберпреступлений совершаются в рамках той или иной формы организованной деятельности, включая формирование черного рынка киберпреступности, основанного на цикле разработки вредоносного программного обеспечения, заражения компьютеров, управления бот-сетями, сбора данных личного и финансового характера, их продажи и получения денег за финансовую информацию. В развитых странах доля киберпреступлений с транснациональным компонентом, выявляемых правоохранительными органами, как правило, высока, тогда как в развивающихся странах она значительно ниже и в некоторых случаях составляет менее 10 %. С одной стороны, это может указывать на то, что в развивающихся странах киберпреступления ориентированы преимущественно на жертв внутри страны и, возможно, на национальные компьютерные системы. С другой стороны, не исключено, что недостаточный уровень развития потенциала правоохранительных органов развивающихся стран приводит к более редкому выявлению преступлений с иностранным элементом или взаимодействию с иностранными поставщиками услуг и жертвами.

Одно из ключевых положений доклада Европола «Оценка угрозы организованной преступности в сфере интернет-технологий» (iОСТА) гласит, что «отличительной чертой структуры киберпреступных групп является полный отрыв от традиционной концепции организованных преступных групп в части, касающейся иерархичности структуры». Хотя это справедливо для большинства случаев, необходимо учитывать широкий спектр типологий, включая динамику преступной деятельности, осуществляемой как в онлайн-, так и в офлайн-режиме. Природа киберпреступлений зачастую требует привлечения значительных средств и человеческих ресурсов. Организованные структуры, созданные с целью совершения киберпреступлений для получения финансовой выгоды (например, хищения банковских реквизитов и номеров кредитных карт), стали объектом наиболее пристального анализа. «Черный рынок» киберпреступности характеризуется высокой степенью взаимодействия групп и частных лиц, выполняющих различные, а иногда и множественные роли («программистов», «распространителей», «технических специалистов», «хакеров», «мошенников», «хостеров», «обналичивателей средств», «денежных курьеров», «кассиров» и «лидеров») в процессе создания вредоносного программного обеспечения, заражения компьютеров (в частности, посредством фишинга по электронной почте), управления бот-сетями, сбора персональных и финансовых данных, продажи сведений и получения денег за финансовую информацию.

По мнению Н.А. Марочкина, демографические характеристики преступников зеркально отражают особенности обычного уголовного мира в том аспекте, что в этой среде преобладают молодые люди мужского пола, хотя возрастной состав все в большей степени свидетельствует об увеличении числа лиц пожилого возраста, особенно когда преступления связаны с детской порнографией. Наряду с тем, что определенная часть преступников может иметь высокий уровень образования, особенно в сфере компьютерных наук, многие из известных правоохранительным органам преступников не имеют специальной подготовки. В нашей стране портрет киберпреступника можно составить на примере одного уголовного дела.

27 января 2017 года приговором районного суда № 2 Бостандыкского района города Алматы граждане О., Д. и 18 лиц признаны виновными в создании, руководстве и участии в организованной группе; создании, использовании и распространении вредоносных программных продуктов; неправомерном завладении информацией; краже денежных средств со счетов физических и юридических лиц в особо крупном размере [2].

В начале 2015 года О. приобрел у Д. через сеть Интернет программный код сайта «K.kz». Поскольку О. разбирался в вирусных программах, а Д. умел осуществлять рассылки спама, они решили похитить денежные средства со счетов компаний путем рассылки вредоносного программного обеспечения. Через сеть Интернет они арендовали серверы: в Соединенном Королевстве Великобритании и Северной Ирландии (IP-адреса: 37.220.20.66, 37.220.20.67, 37.220.20.69, 37.220.20.70, 87.236.211.140); в Федеративной Республике Германия (IP-адреса: 178.162.207.104, 5.61.34.134); во Французской Республике (IP-адрес: 178.32.144.104); в Королевстве Нидерландов (IP-адреса: 95.211.203.121, 31.204.154.148); в Соединенных Штатах Америки (IP-адрес: 46.21.153.4).

25 февраля 2015 года О. и Д., используя электронный адрес xxx@gmail.com, приобрели у компании «Nemoru Software» программный продукт NanoCore, оплатив его через платежную систему PayPal со своего аккаунта. Далее О. и Д. через сеть Интернет приобрели у третьих лиц программы для шифрования и внесли изменения в алгоритм программного продукта NanoCore, дополнив его фрагментами кода для затруднения обнаружения системами защиты компьютеров. Модифицированный программный продукт обеспечивал возможность скрытой установки и

удаленного доступа к зараженному компьютеру.

Учитывая выявленные в стране формы организованных преступных групп, можно предположить, что организованные группы или сообщества могут контролировать деятельность лиц, обладающих познаниями в информационных технологиях, в момент совершения киберпреступлений. Однако даже в таких структурах лица, обладающие познаниями в области информационных технологий, занимают далеко не последние ступени в иерархии преступных групп в силу своей профессиональной компетентности.

Меры борьбы с киберпреступностью, принимаемые в порядке реагирования на совершенные преступления, должны сопровождаться целенаправленными и долгосрочными тактическими расследованиями в отношении преступных рынков и разработчиков преступных схем. Правоохранительные органы развитых стран работают в этой области, в том числе используя действующие под прикрытием подразделения по выявлению правонарушителей на сайтах социальных сетей, в чатах, при обмене мгновенными сообщениями и использовании материалов совместного пользования (P2P). Трудности при расследовании киберпреступлений связаны с использованием преступниками новаторских методов, сложностями в получении доступа к электронным доказательствам, а также с внутренними ограничениями в отношении ресурсов, кадрового потенциала и материально-технической базы. Подозреваемые часто применяют технологии анонимизации и запутывания следов, при этом новые технологии быстро распространяются в преступной среде благодаря функционированию онлайн-преступных рынков.

Заключение

В результате проведенного исследования установлено, что транснациональная киберпреступность представляет собой одну из наиболее динамично развивающихся и сложных угроз современной безопасности, характеризующуюся высокой латентностью, технологичностью и отсутствием территориальных границ. Указанные особенности существенно осложняют деятельность правоохранительных и специальных государственных органов Республики Казахстан по ее выявлению, пресечению и расследованию.

Анализ действующего законодательства и практики его применения показал, что в Республике Казахстан сформирована определенная правовая и институциональная база противодействия киберпреступности. Вместе с тем выявлен ряд проблем, связанных с необходимостью дальнейшей адаптации национального законодательства к международным стандартам, совершенствования механизмов межведомственного взаимодействия, а также расширения международного сотрудничества в условиях транснационального характера киберугроз.

Установлено, что эффективность борьбы с транснациональной киберпреступностью во многом зависит от уровня технической оснащенности правоохранительных органов, квалификации кадров, а также оперативности обмена информацией как внутри страны, так и на международном уровне. В этой связи особое значение приобретают развитие специализированных подразделений, внедрение современных цифровых технологий и повышение уровня профессиональной подготовки сотрудников.

По результатам исследования обоснована необходимость:

- дальнейшего совершенствования нормативно-правовой базы в сфере кибербезопасности;
- усиления международного сотрудничества, включая участие в профильных конвенциях и совместных операциях;
- развития механизмов межведомственного и межгосударственного обмена информацией;
- внедрения современных методов цифровой криминалистики и аналитики;
- повышения уровня киберграмотности и профессиональной подготовки сотрудников правоохранительных и специальных органов.

Таким образом, противодействие транснациональной киберпреступности требует комплексного, системного и междисциплинарного подхода, основанного на тесном взаимодействии государственных органов, международных организаций и научного сообщества. Реализация предложенных мер позволит повысить эффективность деятельности правоохранительных и специальных государственных органов Республики Казахстан и укрепить национальную безопасность в условиях цифровой трансформации.

Список литературы

1. Номоконов В.А. Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра, 2012. – № 1 (24). – С. 45-55.
2. Марочкин Н.А. Алгоритмизация – эффективный метод оптимизации расследования преступлений // Известия Алтайского государственного университета, 2001. – №2. – С. 45-49.

References

1. Nomokonov V.A. Kiberprestupnost' kak novaya kriminal'naya ugroza // Kriminologiya: vchera, segodnya, zavtra, 2012. – № 1 (24). – S. 45-55.
2. Marochkin N.A. Algoritmizatsiya – effektivnyy metod optimizatsii rassledovaniya prestupleniy // Izvestiya Altayskogo gosudarstvennogo universiteta, 2001. – №2. – S. 45-49.

Н.М. Батырбай¹, Н.Д. Тлешалиев²

¹PhD доктор, Каспий қоғамдық университетінің «Әділет» Жоғары заң мектебі деканының орынбасары (Алматы қ., Қазақстан)
e-mail: nurbol.ansar2019@gmail.com; ORCID ID: 0000-0002-9679-2262

²PhD доктор, Қазақстан Республикасы Мемлекеттік қызмет істері агенттігінің Алматы қаласы бойынша департаментінің Сыбайлас жемқорлықтың алдын алу басқармасының басшысы,
(Алматы қ., Қазақстан)
e-mail: ali_2301@mail.ru; ORCID ID: 0000-0003-3871-866X

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ ҚҰҚЫҚ ҚОРҒАУ ЖӘНЕ АРНАУЛЫ МЕМЛЕКЕТТІК ОРГАНДАРЫНЫҢ ҚЫЗМЕТКЕРЛЕРІМЕН ТРАНСҰЛТТЫҚ КИБЕРҚЫЛМЫСҚА ҚАРСЫ КҮРЕС

Аңдатпа

Мақалада Қазақстан Республикасының Құқық қорғау және арнаулы мемлекеттік органдары қызметкерлерінің трансұлттық киберқылмысқа қарсы күрестің өзекті мәселелері қарастырылды. Цифрландыру және жаһандану жағдайында киберқылмыстың арту ерекшеліктері мен үрдістері талданды, сондай-ақ оның алдын алу, анықтау және тергеу кезінде туындайтын негізгі проблемалар анықталды. Қазақстан Республикасының қолданыстағы заңнамасын талдауға және оның киберқауіптерге қарсы іс-қимыл саласындағы халықаралық стандарттарға сәйкестігіне ерекше назар аударылды. Ақпарат алмасуды және бірлескен операцияларға қатысуды қоса алғанда, ведомствоаралық өзара іс-қимыл және халықаралық ынтымақтастық мәселелері қаралды.

Зерттеу барысында жүйелік, салыстырмалы-құқықтық, статистикалық және ресми-құқықтық талдауды қоса алғанда, жалпы ғылыми және арнайы әдістер қолданылды. Жүргізілген зерттеу негізінде нормативтік-құқықтық базаны жетілдіруге, құқық қорғау және арнайы органдар қызметінің тиімділігін арттыруға, цифрлық технологияларды дамытуға және халықаралық өзара іс-қимылды нығайтуға бағытталған ұсыныстар тұжырымдалды.

Құқықтық, ұйымдастырушылық және технологиялық шараларды қамтитын трансұлттық киберқылмысқа қарсы іс-қимылға кешенді көзқарастың қажеттілігі туралы қорытынды жасалды. Сондай-ақ, мақалада трансұлттық киберқылмыспен күресу практикасына талдау жасалып, оның негізінде негізгі кезеңдер, проблемалар анықталып, оларды шешу жолдары ұсынылды. Киберқауіптердің таралуы мен қоғамдық қауіптілігінің артуына байланысты көптеген отандық және шетелдік зерттеушілер бұл мәселеге алаңдайды.

Түйін сөздер: трансұлттық киберқылмыс, қылмысқа қарсы іс-қимыл, қылмыстың алдын алу, Ұлттық қауіпсіздік, құқық қорғау органдары, қылмыс, шаралар.

N.M. Batyrbay¹, N.D. Tleshaliyev²

¹PhD, Deputy Dean of the Higher School of Law «Adilet» of the
Caspian Public University, (Almaty, Kazakhstan)

ORCID ID: 0000-0002-9679-2262; e-mail: nurbol.ansar2019@gmail.com

²PhD, Head of the Department for Corruption Prevention of the Department of
the Agency of the Republic of Kazakhstan for Civil Service Affairs in Almaty,
(Almaty, Kazakhstan)

ORCID ID: 0000-0003-3871-866X; e-mail: ali_2301@mail.ru

COMBATING TRANSNATIONAL CYBERCRIME BY LAW ENFORCEMENT AND SPECIAL GOVERNMENT AGENCIES OF THE REPUBLIC OF KAZAKHSTAN

Abstract

The article discusses topical issues of combating transnational cybercrime by law enforcement officers and special government agencies of the Republic of Kazakhstan. The features and trends of cybercrime development in the context of digitalization and globalization are analyzed, as well as key problems arising in its prevention, detection and investigation are identified. Special attention is paid to the analysis of the current legislation of the Republic of Kazakhstan and its compliance with international standards in the field of countering cyber threats. The issues of interagency cooperation and international cooperation, including information exchange and participation in joint operations, were considered.

The research uses general scientific and special methods, including systematic, comparative legal, statistical and formal legal analysis. Based on the conducted research, proposals have been formulated aimed at improving the regulatory framework, increasing the effectiveness of law enforcement and special agencies, developing digital technologies and strengthening international cooperation.

It is concluded that there is a need for an integrated approach to countering transnational cybercrime, including legal, organizational and technological measures. The article also analyzes the practice of combating transnational cybercrime, on the basis of which the main stages, problems are identified and ways to solve them are proposed. Due to the prevalence and increased public danger of cyber threats, many domestic and foreign researchers are concerned about this issue.

Keywords: transnational cybercrime, crime prevention, crime prevention, national security, law enforcement agencies, crime, measures.