

ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ: ОПЫТ МЕЖДУНАРОДНОГО СОТРУДНИЧЕСТВА

Сатбаева Айжан Муратовна¹

Кандидат юридических наук, доцент кафедры «Социально-гуманитарные науки» Университета Международного Бизнеса имени Кенжегали Сагадиева, г. Алматы, Республика Казахстан, e-mail: sathaeva@mail.ru

Алимбетова Алида Робертиновна

Доктор PHD, доцент кафедры «Экономика, услуги и право» Института «Педагогика, бизнес и право» Алматинского гуманитарно-экономического университета, г. Алматы, Республика Казахстан, e-mail: alimbetova_alida@mail.ru

Бейсенбаева Маншук Токтарбековна

Кандидат юридических наук, ассоциированный профессор кафедры «Право» Казахского национального аграрного исследовательского университета, г. Алматы, Республика Казахстан, e-mail: manshuk.beisenbaeva@mail.ru

Аннотация. Исследование посвящено проблеме противодействия киберпреступности в контексте опыта международного сотрудничества. Выделяется тенденция в процессе происходящей трансформации из постиндустриального в информационное общество: глобальная информатизация и диджитализация процессов приводят к угрозе вмешательства в личную жизнь, краже данных и нарушению конфиденциальности.

Анализ международных правовых актов позволил сделать выводы о необходимости расширения сотрудничества государств в борьбе с киберпреступностью под эгидой ООН на основе программных, стратегических актов международно-правового регулирования соответствующего круга отношений. Отмечается важное значение создания и разработки организационных и законодательных мер противодействия киберпреступности, совершенствование взаимодействия между компетентными органами различных государств.

В исследовании обоснована необходимость разработки и принятия универсальных конвенций по борьбе с киберпреступностью. Авторы статьи констатируют, что масштабный рост объема передачи информации вызывает необходимость обеспечения максимального уровня защиты данных, как самими заинтересованными пользователями ИКТ, так и правительствами- гарантам информационной безопасности государства и стабильности. Международная нормативно-правовая база обеспечивает решение проблемы по трем направлениям: снижение расхождений между национальными законодательствами, введение новых полномочий органов и содействие международному сотрудничеству.

Констатируется, что в Республике Казахстан нет комплексных исследований по борьбе с кибертерроризмом и киберпреступностью, как явлениями, которые включают в себя весь спектр преступлений, которые совершаются сегодня в Интернете. Исследование восполняет данный пробел: анализируется деятельность законодательного и правоприменительных органов Республики Казахстан.

Ключевые слова: киберпреступность, кибербезопасность; международное сотрудничество, международно-правовое регулирование, борьба с киберпреступностью, Конвенция о киберпреступности.

¹ Автор для корреспонденции

КИБЕР ҚЫЛМЫСТЫЛЫҚҚА ҚАРСЫ КҮРЕС ЖҮРГІЗУ МӘСЕЛЕЛЕРІ: ХАЛЫҚАРАЛЫҚ ҮНТЫМАҚТАСТЫҚ ТӘЖІРИБЕСІ

Айжан Мұратқызы Сәтбаева

Заң ғылымдарының кандидаты, Кенжеғали Сағадиев атындағы Халықаралық Бизнес Университетінің «Әлеуметтік-гуманитарлық ғылымдар» кафедрасының доценті, Алматы қ., Қазақстан Республикасы, e-mail: sathaeva@mail.ru

Алида Робертиновна Алимбетова

RHD докторы, Алматы гуманитарлық-экономикалық университетінің «Педагогика, бизнес және құқық» институтының «Экономика, қызметтер және құқық» кафедрасының доценті, Алматы қ., Қазақстан Республикасы, e-mail: alimbetova_alida@mail.ru

Мәншүк Тоқтарбекқызы Бейсенбаева

Заң ғылымдарының кандидаты, Қазақ ұлттық аграрлық зерттеу университетінің «Құқық» кафедрасының қауымдастырылған профессоры, Алматы қ., Қазақстан Республикасы, e-mail: manshuk.beisenbaeva@mail.ru

Аннотация. Зерттеу халықаралық ынтымақтастық тәжірибесі контекстінде киберқылмыспен күрес мәселесіне арналған. Постиндустриалды қоғамнан ақпараттық қоғамға үздіксіз трансформациялау үрдісінде: процестерді жаһандық ақпараттандыру және цифрландыру жеке өмірге араласу қаупі, деректердің ұрлануы және құпиялылықтың бұзылуы тенденциясына әкелетіні анықталды.

Халықаралық құқықтық актілерді талдау өзара қарым-қатынастардың тиісті саласын халықаралық-құқықтық реттеудің бағдарламалық, стратегиялық актілері негізінде Біріккен Ұлттар Ұйымының қамқорлығымен мемлекеттердің киберқылмыстылықпен күресудегі ынтымақтастығын кеңейту қажеттілігі туралы қорытынды жасауға мүмкіндік берді. Киберқылмыстылықпен күресу бойынша ұйымдастырушылық және заңнама-лық шараларды құру мен дамытудың, әртүрлі мемлекеттердің құзыретті органдарының өзара іс-қимылын жақсартудың маңыздылығы.

Зерттеуде киберқылмыспен күрес жөніндегі әмбебап конвенцияларды әзірлеу және қабылдау қажеттілігі негізделген. Мақала авторлары ақпаратты тасымалдау көлемінің ауқымды өсуі мүдделі АКТ пайдаланушылардың өздері де, мемлекеттік ақпараттық қауіпсіздік пен тұрақтылықтың кепілі – үкіметтер де деректерді қорғаудың шекті деңгейін қамтамасыз ету қажеттілігін талап етеді. Халықаралық нормативтік-құқықтық база мәселені үш бағытта шешуді қарастырады: ұлттық заңнамалар арасындағы қайшылықтарды азайту, билік органдарының жаңа өкілеттіктерін енгізу және халықаралық ынтымақтастыққа жәрдемдесу.

Қазақстан Республикасында кибертерроризммен және киберқылмыспен күресу бойынша бүгінгі таңда интернетте жасалып жатқан қылмыстардың барлық кешенін қамтитын құбылыс ретінде кешенді зерттеулер жүргізілмегені дәйектеледі. Зерттеу Қазақстан Республикасының заң шығарушы және құқық қорғау органдарының қызметіне талдау жасай отырып осы олқылықтың орнын толтырады.

Түйінді сөздер: киберқылмыс, киберқауіпсіздік, халықаралық ынтымақтастық, халықаралық-құқықтық реттеу, киберқылмыспен күрес, Киберқылмыстар туралы конвенция.

CYBERCRIMECHALLENGES: EXPERIENCE OF INTERNATIONAL COOPERATION

Satbayeva Aizhan Muratovna

Candidate of Legal Sciences, Associate Professor of the Department of Social and Humanities Sciences, Kenzhegali Sagadiyev University of International Business, Almaty, Republic of Kazakhstan, e-mail: sathaeva@mail.ru

Alimbetova Alida Robertinovna

Doctor PHD, Associate Professor, Department of Economics, Services and Law, Institute of Pedagogy, Business and Law, Almaty University of Humanities and Economics, Almaty, Republic of Kazakhstan, e-mail: alimbetova_alida@mail.ru

Beissenbayeva Manshuk Toktarbekovna

Candidate of Legal Sciences, Associate Professor of the Department of Law, Kazakh National Agrarian Research University, Candidate of Legal Sciences, Almaty, Republic of Kazakhstan, e-mail: manshuk.beisenbaeva@mail.ru

Abstract. *The study focuses on the problem of countering cybercrime in the context of the experience of international cooperation. The trend in the process of ongoing transformation from a post-industrial to an information society stands out: global informatization and digitalization of processes lead to the threat of interference in personal life, data theft and violation of privacy.*

The analysis of international legal acts made it possible to draw conclusions about the need to expand cooperation between states in the fight against cybercrime under the auspices of the UN on the basis of programmatic, strategic acts of international legal regulation of the relevant range of relations. The importance of creating and developing organizational and legislative measures to combat cybercrime, improving interaction between the competent authorities of various states.

The study justified the need to develop and adopt universal conventions to combat cybercrime. The authors of the article state that the large-scale growth in the volume of information transfer causes the need to ensure the maximum level of data protection, both by the interested ICT users themselves and by governments - guarantors of state information security and stability. The international legal framework provides a solution to the problem in three areas: reducing discrepancies between national laws, introducing new powers of bodies and promoting international cooperation.

It is stated that in the Republic of Kazakhstan there are no comprehensive studies on combating cyberterrorism and cybercrime as phenomena that include the entire range of crimes that are committed today on the Internet. The study fills this gap: the activities of the legislative and law enforcement bodies of the Republic of Kazakhstan are analyzed.

Keywords: *cybercrime; cybersecurity; international cooperation; international legal regulation; combating cybercrime; Convention on Cybercrime.*

DOI: 10.52026/2788-5291_2024_78_3_211

Введение

Активное внедрение современных информационных технологий в различные сферы, включая государственные и частные структуры, а также в обществе в целом, требует решения возникших проблем информационной безопасности. Возможность несанкционированного доступа к информации, ее модификация или уничтожение, представляют серьезную угрозу для государственной безопасности и прав человека в целом [1, с.123]. Один из способов установления более эффективной правовой основы в борьбе с уголовными правонарушениями в области высоких технологий заключается в анализе международных правовых норм. [2, с.360].

Такие общественно опасные действия, как создание различных вредоносных программ, различных игр для детей со смертельным исходом, взлом банковских счетов, мошенничество с банковскими картами, Интернет-терроризм – получили довольно

распространённое название «киберпреступления».

Европол (2018) разделяет киберпреступления «на киберзависимые преступления (т.е. любое преступление, которое может быть совершено только с использованием компьютеров, компьютерных сетей или других форм информационно-коммуникационных технологий) и преступления, совершаемые посредством кибертехнологий (т.е. традиционные преступления, совершаемые с помощью Интернета и цифровых технологий). Ключевое различие между этими категориями киберпреступности заключается в роли информационно-коммуникационных технологий в совершении правонарушения – являются ли ИКТ целью преступления или неотъемлемой частью способа совершения преступления, использованного преступником. Когда ИКТ являются целью преступления, такие киберпреступления негативно влияют на конфиденциальность,

целостность и/или доступность компьютерных данных или систем»².

В современных условиях ООН взяла на себя координирующую роль в разработке как концептуальных, так и правовых основ регулирования ключевых вопросов в сфере борьбы с киберпреступностью. Характер и тяжесть совершенных преступлений требует немедленной реакции международного сообщества на соответствующие негативные социальные проявления. Именно под эгидой ООН, которая объединяет наибольшее количество государств мира, целесообразно проводить деятельность по разработке и внедрению международно-правового регулирования исследуемых общественных отношений. Принятие соответствующей резолюции, которая обозначила рамочные договоренности, стало одним из первых шагов на пути к созданию международно-правовой базы по проблематике борьбы с киберпреступностью [3].

В 1997 году между министрами юстиции и министрами внутренних дел стран Большой Восьмерки в Вашингтоне были разработаны и подписаны «Десять принципов борьбы с высокотехнологичными преступлениями», которые, в частности, включают в себя положение о том, что для лиц, злоупотребляющих информационными технологиями, не должно быть никаких зон безопасности. Так, правовая система должна обеспечивать конфиденциальность, целостность и пригодность данных и систем, и защищать от преступного повреждения и гарантировать наказание за серьезные правонарушения [4, с.30]. Конференция составила повестку дня для последующей встречи на высшем уровне, проведенной в 22 июля 2000 года в Японии на о. Окинава [2, с.262].

18 января 2013 г. в Гааге официально открыт Европейский центр по борьбе с киберпреступностью. Целями его создания являются сбор и обработка данных по киберпреступлениям, проведение экспертных оценок Интернет-угроз, разработка и внедрение передовых методов профилактики и расследования киберпреступлений, подготовка новых кадров, оказание помощи правоохранительным и судебным органам, а также координация совместных действий заинтересованных сторон, направленных на повышение уровня безопасности в европейском киберпространстве [5, с.372].

Особенностями универсального международно-правового регулирования борьбы с киберпреступностью является следующее: 1) соответствующая деятельность аккумулируется вокруг ООН и ее органов или созданных при ее поддержке субъектов [6]; 2) на сегодня имеются исключительно программные и другие стратегические документы, которые должны заложить основы международно-правового регулирования соответствующего круга отношений [7]; 3) основными направлениями деятельности должно быть создание и разработка организационных и законодательных мер противодействия киберпреступности, а также вопросы взаимодействия в данной сфере деятельности; 4) имеется необходимость в создании международных совместных органов оперативно-розыскной деятельности для обеспечения фиксирования следов совершенных преступлений; 5) совершенствование взаимодействия между компетентными органами различных государств [8]. Кроме того, существует настоятельная необходимость разработки и принятия универсальных конвенций по соответствующим вопросам, которые бы обеспечили участие большинства государств в соответствующих мероприятиях против киберпреступности [9].

Важно осознавать, что киберпреступность является всемирной проблемой. Кибератаки могут парализовать как частные организации, так и государственные структуры, и нет сейчас в мире государства, которое было бы полностью защищено от подобных атак. Вероятными источниками киберугроз являются не только хакеры или их группы, но также и отдельно взятые государства, преступные группировки и террористические организации. Во время разработки способов и методов борьбы с киберпреступностью нужно учитывать латентность данного рода преступлений. Эксперты оценивают латентность киберпреступлений крайне высоко: 80 % - в США, 75 % - в Германии, в Великобритании - 85 %, а в России - более чем 90 % [5, с.374].

Если обратиться в статистике уголовных дел по Республике Казахстан, то согласно данным Генеральной прокуратуры, в 2022 году зарегистрировано всего 85 таких правонарушений, а в первом полугодии 2023 года - 43 [10]. Чаще всего дела возбуждались по статье 205 Уголовного кодекса Республики

² Введение в киберпреступность. Модуль 1. Управление Организации Объединенных Наций по наркотикам и преступности. ООН, Вена, 2019. // https://www.unodc.org/documents/e4j/Cybercrime/Cybercrime_Module_1_Introduction_to_Cybercrime_RU.pdf. (датаобращения 16.12.2023).

Казахстан. На втором месте по количеству возбужденных дел статья 206 Уголовного кодекса Республики Казахстан. В 2022 году было зафиксировано 15 таких дел, за первое полугодие 2023 – 14 [10].

Как отмечают российские исследователи Приходько Д.В., Белькова А.А. «по мнению ведущего исследователя кибербезопасности агентства Cybersecurity Ventures, самым быстрорастущим типом киберпреступности становятся программы-вымогатели. Ожидается, что в 2021 г. компании будут подвергаться этому типу киберпреступлений каждые 11 секунд, по сравнению с 14 секундами в 2019 г. и 40 секундами в 2016 г.» [11, с.92].

Вышеуказанные факты говорят о выходе покушений в сфере Интернет-технологий за пределы уровня феномена и свидетельствуют о необходимости выделения самостоятельного вида преступлений – киберпреступлений, и такого опасного явления как киберпреступность с присущими ей признаками, особенностями, а также подтверждают актуальность дальнейших исследований в сфере борьбы с киберпреступностью.

Эффективность противодействия явлению киберпреступности видится в совместных действиях государственного и частного секторов, совершенствовании международного и национального законодательства, организации международных подразделений и структур в борьбе с киберпреступностью. Что касается Казахстана, то пока ещё нет комплексных исследований по борьбе с кибертерроризмом и киберпреступностью как явлениями, которые включают в себя весь спектр преступлений, которые совершаются сегодня в Интернете. Исследования по противодействию киберпреступности, особенно в контексте международного измерения, и рассмотрение киберпреступности как глобального явления в настоящее время в основном проводятся исключительно зарубежными учеными. В то же время они, естественно, не охватывают аспекты казахстанского законодательства. Таким образом, целью исследования является поиск действенного механизма контроля киберпреступности в мире.

Материалы и методы

Проведен комплексный анализ международных методов борьбы с киберпреступностью на основе их эффективности, современности и масштаба. Были изучены основные

результаты противодействия этому явлению на законодательном уровне, а также пути повышения информационной безопасности в разных странах. При изучении поставленной проблемы были использованы законодательные и другие нормативно-правовые акты Республики Казахстан. Кроме того, было проанализировано Соглашение о сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации. В целях понимания перспектив искоренения киберпреступности, были изучены международные договоры, акты, изданные международными институтами, нормативные акты стран Европы, США. Особое внимание было уделено роли ООН в борьбе с киберпреступностью.

Методологический пласт исследования базируется на общенаучных и специальных научных методах. Применение метода формальной логики позволило систематизировать существующие понятия и факты, имеющие отношение к проблеме киберпреступности. Использование системно-функционального метода предоставило возможность для рассмотрения исследуемого объекта как явления планетарного масштаба в целом и в рамках отдельных государств, в том числе и в Республике Казахстан. В исследовании широко использованы методы компаративистики, документального анализа международно-правовых актов и актов национального права, контент-анализа интернет-источников, ситуационного анализа и прогнозирования, правового моделирования.

Результаты

Важные вопросы сотрудничества государств в борьбе с преступным использованием информационно-коммуникационных технологий было возложено на Международный союз электросвязи. Впоследствии на выполнение запланированных мероприятий был принят ряд резолюций МСЭ, которые направлены на борьбу с компьютерными преступлениями³.

Конвенция Совета Европы о киберпреступности, принятая в Будапеште 23 ноября 2001 года, стала логическим продолжением этой резолюции ООН и плодом многолетних усилий международного сообщества [2, с.362]. Значение данного международного нормативно-правового акта можно выразить следующим образом. Во-первых, Кон-

³ Регламент международной электросвязи (РМЭ) // [https://www.itu.int/ru/wcit-12/Pages/itrs.aspx\(датаобращения16.12.2023\)](https://www.itu.int/ru/wcit-12/Pages/itrs.aspx(датаобращения16.12.2023))

венцией осуществлено разграничение киберпреступлений в зависимости от объекта посягательства на: 1) преступления против конфиденциальности, целостности и доступности компьютерных данных и систем, 2) правонарушения, связанные с компьютерами, 3) правонарушения, связанные с содержанием, 4) правонарушения, связанные с нарушением авторских и смежных прав [12, с.772]. Похожим образом классифицируют такие правонарушения и в национальных законодательствах стран-участниц Конвенции. Во-вторых, Конвенцией регламентированы процедурные аспекты, такие как условия, меры пресечения, обыск и арест хранимых компьютерных данных, сбор данных о движении в режиме реального времени, перехват данных, содержащих информацию, юрисдикция и тому подобное. Такая систематизация значительным образом облегчает деятельность правоохранительных органов государства. В-третьих, данным документом установлены принципы сотрудничества стран-участниц в сфере борьбы с киберпреступностью⁴, в частности - экстрадиции и взаимопомощи. Следует отметить, что реализация этого аспекта осуществляется путем заключения государствами двусторонних соглашений. Как уже показал их анализ, на практике страны-участницы предпочитают реализацию принципа взаимопомощи [13]. В-четвертых, Конвенция дает право участникам осуществлять доступ к публично доступным компьютерным данным, не получая разрешения от другой стороны, что значительным образом облегчает расследование преступлений и позволяет избегать чрезмерного затягивания оперативно-розыскной деятельности.

Среди международных договоров против киберпреступности, следует отметить Соглашение о сотрудничестве государств-участников СНГ в борьбе с преступлениями в сфере компьютерной информации от 01 июня 2001 года. Это соглашение возлагает на государства обязательства по признанию в соответствии с национальным законодательством в качестве уголовных преступлений: 1) осуществление неправомерного

доступа к компьютерной информации, охраняемой законом, если это повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети; 2) создание, использование или распространение вредоносных программ; 3) нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системы ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию информации ЭВМ, охраняемой законом, если это повлекло существенный вред или тяжкие последствия; 4) противозаконное использование программ для ЭВМ и баз данных, являющихся объектами авторского права, так же как и присвоение авторства⁵.

Однако для полноценной реализации соответствующих задач необходимо было согласовать четкий перечень соответствующих преступных деяний и наказания за них. На практике не все государства, которые являются участниками СНГ, реализовали соответствующие задачи, что существенно снижает противодействие информационной преступности, которая требует комплексного транснационального сотрудничества.

В последние годы были разработаны и приняты несколько важных документов, направленных на усиление правового регулирования и улучшение международного сотрудничества в борьбе с киберпреступностью. К таким документам относятся:

1. Рекомендательные типологии новых преступлений, совершаемых с использованием информационных технологий, от 27 ноября 2020 года предоставляют типовые формы новых киберпреступлений, что способствует их лучшей идентификации и классификации. Примеры таких преступлений включают фишинг, мошенничество с использованием криптовалют и атаки на системы искусственного интеллекта⁶. Следовательно, предлагаемая типология преступлений имеет важное значение для унификации подходов к классификации киберпреступлений, что облегчает международное сотрудничество в их расследовании и предотвращении.

2. Рекомендации о доступе к информации

⁴ *Combating Cybercrime Tools and Capacity Building for Emerging Economies* // <https://www.itu.int/en/ITU-D/Cybersecurity/Documents/worldbank-combating-cybercrime-toolkit.pdf> (дата обращения 16.12.2023).

⁵ Указ Президента Республики Казахстан от 25 июня 2002 года N 897 «Об утверждении Соглашения о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации» // https://adilet.zan.kz/rus/docs/U020000897_ (дата обращения 16.12.2023).

⁶ Рекомендательные типологии новых преступлений, совершаемых с использованием информационных технологий. Приложение к постановлению МПА СНГ от 27 ноября 2020 года № 51-24 // https://iacis.ru/baza_dokumentov/modelnie_zakonodatelnie_akti_i_rekomendacii_mpa_sng/vspomogatelnie_pravovie_akti_i_zakonoproektnie_predlozheniya (дата обращения 16.12.2023).

о правовом статусе граждан от 16 апреля 2021 года направлены на улучшение доступа граждан к правовой информации, что важно для защиты их прав в цифровой среде. Включают меры по обеспечению прозрачности и доступности правовой информации через цифровые платформы⁷. На наш взгляд, увеличение доступности правовой информации будет способствовать повышению правовой грамотности населения, что, в свою очередь, может уменьшить число преступлений, связанных с неосведомленностью граждан о своих правах.

3. В рекомендациях о сотрудничестве государств - участников СНГ в сфере цифрового развития от 26 ноября 2021 года акцентируется внимание на мерах по улучшению сотрудничества в области цифрового развития, включая совместные усилия в борьбе с киберпреступностью, обмен информацией и координацию действий между государствами⁸. Из этого следует, что совместные усилия в цифровом развитии и обмен опытом между государствами СНГ помогут создать более устойчивую и защищенную цифровую среду, что будет способствовать снижению рисков киберпреступлений на межгосударственном уровне.

4. Модельный закон о противодействии киберпреступности от 14 апреля 2023 года разработан для предоставления стандартизированных законодательных мер государствам СНГ, с целью эффективного противодействия киберпреступлениям. Включает положения о повышении ответственности за киберпреступления и усилении наказаний за их совершение⁹. Внедрение данного модельного закона будет способствовать гармонизации законодательства государств СНГ в области кибербезопасности, что, в свою очередь, повысит эффективность транснационального сотрудничества в борьбе с киберпреступностью.

Для более полной картины можно также

рассмотреть данные нового ежегодного исследования восприятия глобальных рисков (Global Risks Perception Survey - GRPS), проводимого Всемирным экономическим форумом (2023-2024 гг.), где киберпреступность выделена как одна из наиболее значимых угроз в ближайшие годы.

Рассмотрим основные моменты, связанные с киберпреступностью.

Во-первых, киберугрозы занимают 4-е место среди краткосрочных рисков на горизонте до двух лет. Это свидетельствует о серьезной угрозе, которую киберпреступность представляет для глобальной безопасности и стабильности¹⁰.

Во-вторых, технологические вызовы продолжают нарастать. Развитие таких технологий, как генеративный ИИ и квантовые вычисления, способствует росту киберугроз. Эти передовые технологии активно используются злоумышленниками для создания более сложных атак и расширения числа потенциальных целей. В результате, защита от таких угроз требует постоянного обновления и совершенствования средств кибербезопасности¹¹. Кроме того, увеличивается разрыв в киберустойчивости между различными организациями. Те, кто может позволить себе инвестировать в современные средства защиты, находятся в более выгодном положении по сравнению с теми, у кого таких возможностей нет. Это делает всех участников цифровой экосистемы более уязвимыми, даже тех, кто лучше защищен¹².

В-третьих, не следует недооценивать социальные последствия киберпреступности. По мнению экспертов, в 2024 году ожидается рост социального неравенства из-за киберугроз. Например, в Юго-Восточной Азии более 220 000 человек были вовлечены в онлайн-мошенничество, что свидетельствует о значительных социально-экономических последствиях киберпреступности¹³.

⁷ Рекомендации «О доступе к информации о правовом статусе граждан». Приложение к постановлению МПА СНГ от 16 апреля 2021 года № 52-7 // https://iacis.ru/ob_organizacii/struktura_mpa_sng/postoyannie_komissii_mpa_sng/komissiya_po_sotsialnoj_politike_i_pravam_cheloveka (дата обращения 16.12.2023).

⁸ Рекомендации «О доступе к информации о правовом статусе граждан». Приложение к постановлению МПА СНГ от 16 апреля 2021 года № 52-7 // https://iacis.ru/ob_organizacii/struktura_mpa_sng/postoyannie_komissii_mpa_sng/komissiya_po_sotsialnoj_politike_i_pravam_cheloveka (дата обращения 16.12.2023).

⁹ Модельный закон «О противодействии киберпреступности». Приложение к постановлению МПА СНГ от 14.04.2023 № 55-20 // https://iacis.ru/baza_dokumentov/modelnie_zakonodatelnie_akti_i_rekomendacii_mpa_sng/modelnie_kodeksi_i_zakoni (дата обращения 16.12.2023).

¹⁰ Global Risks Report 2024 // <https://www.weforum.org/publications/global-risks-report-2024/> (дата обращения 16.12.2023).

¹¹ Global Risks Report 2024: The risks are growing — but so is our capacity to respond // <https://www.weforum.org/agenda/2024/01/global-risk-report-2024-risks-are-growing-but-theres-hope/> (дата обращения 16.12.2023).

¹² Global Risks Report 2024: The risks are growing — but so is our capacity to respond // <https://www.weforum.org/agenda/2024/01/global-risk-report-2024-risks-are-growing-but-theres-hope/> (дата обращения 16.12.2023).

¹³ Global Risks Report 2024: The risks are growing — but so is our capacity to respond // <https://www.weforum.org/agenda/2024/01/global-risk-report-2024-risks-are-growing-but-theres-hope/>

В-четвертых, в некоторых регионах наблюдается слияние киберпреступности и насильственных преступлений, что усугубляет проблему безопасности. Это явление требует внимания и разработки новых стратегий борьбы с такими комбинированными угрозами¹⁴.

В-пятых, быстрое развитие ИИ представляет собой дополнительные риски, поскольку технологии могут использоваться для создания ложной информации, способствуя дезинформации и социальным конфликтам. Эти риски требуют разработки и внедрения надежных мер регулирования и управления¹⁵.

Как отмечают авторы доклада, для борьбы с киберугрозами требуются совместные усилия и инвестиции в области кибербезопасности. Поддержка наименее защищенных организаций принесет пользу всем, так как кибератаки часто касаются не только конкретных целей, но и могут иметь более широкие последствия¹⁶.

Таким образом, для эффективного противодействия киберпреступности необходимо учитывать не только технологические аспекты, но и социальные последствия, а также необходимость международного сотрудничества и совместных усилий в этой области.

Согласно исследованию «Global Cyber security Index 2023», по состоянию на июль 2023 года Малайзия достигла самого высокого балла по национальному индексу кибербезопасности среди стран Азиатско-Тихоокеанского региона-79,22 балла из 100¹⁷. В рейтинге стран по национальному индексу кибербезопасности Казахстан на 31 августа 2023 года занял 78-е место из 176 в мире. Индекс РК составил 48,05% (максимально возможный - 100%), уровень цифрового развития населения достиг 60,18%. Первое место занимает Бельгия - 94,81¹⁸.

Следовательно, можно утверждать, что

важность и актуальность вопросов кибербезопасности в Казахстане остаются на высоком уровне. Важно отметить, что применяемые методы противодействия киберпреступности продемонстрировали свою эффективность, подчеркивая их релевантность.

Стоит сказать и о позитивных моментах, которые существуют в законодательстве Казахстана. Например, управление «К», созданное в Министерстве внутренних дел (МВД) Казахстана в апреле 2003 г., ведет борьбу с широким спектром преступлений, связанных с компьютерными и Интернет-технологиями, включая кибербуллинг, производство контрафактных видеодисков, распространение информации, способствующей экстремизму, терроризму, жестокости и насилию.

Глава 7 Уголовного кодекса Республики Казахстан посвящена уголовным правонарушениям в сфере информатизации и связи¹⁹. Постановлением Правительства Республики Казахстан была утверждена Концепция кибербезопасности ("Киберцит Казахстана")²⁰. В 2023 году в рамках пилотного проекта в Казахстане запустили специальное киберподразделение полиции «Ударно-целевая группа Киберпол», основной задачей которого является защита граждан и бизнеса страны от киберугроз²¹.

Обсуждение

Вместе с тем, несмотря на множество региональных международных договоров по борьбе с киберпреступностью, нет такого глобального акта, который бы удовлетворил всех участников международного сообщества.

В 2017 году члены BRICS вновь заявили о своем желании создать универсальный нормативно-правовой общеобязательный документ по борьбе с преступным использованием ИКТ под эгидой ООН. Так, некоторые

global-risk-report-2024-risks-are-growing-but-theres-hope/ (дата обращения 16.12.2023).

¹⁴ *Global Risks Report 2024: Three risks we aren't talking enough about* // <https://www.weforum.org/agenda/2024/02/emerging-global-risks-report-2024-crime-censorship/> (дата обращения 16.12.2023).

¹⁵ *Global Risks Report 2024: Three risks we aren't talking enough about* // <https://www.weforum.org/agenda/2024/02/emerging-global-risks-report-2024-crime-censorship/> (дата обращения 16.12.2023).

¹⁶ *Global Risks Report 2024: The risks are growing — but so is our capacity to respond* // <https://www.weforum.org/agenda/2024/01/global-risk-report-2024-risks-are-growing-but-theres-hope/> (дата обращения 16.12.2023).

¹⁷ *National cyber security index ranking in the Asia-Pacific region as of July 2023* // <https://www.statista.com/statistics/1400043/apac-national-cyber-security-index-ranking-by-country/> (дата обращения 16.12.2023).

¹⁸ *В рейтинге стран по национальному индексу кибербезопасности Казахстан занял 78-е место из 176* // <https://ranking.kz/rankings/industries-rankings/v-reytinge-stran-po-natsionalnomu-indeksu-kiberbezopasnosti-kazahstan-zanyal-78-e-mesto-iz-176.html> (дата обращения 16.12.2023).

¹⁹ *Уголовный кодекс Республики Казахстан от 3 июля 2014 года № 226-V ЗРК* // <https://adilet.zan.kz/rus/docs/K1400000226> (дата обращения 16.12.2023).

²⁰ *Постановление Правительства Республики Казахстан от 30 июня 2017 года № 407 «Об утверждении Концепции кибербезопасности («Киберцит Казахстана»)»* // <https://adilet.zan.kz/rus/docs/P1700000407> (дата обращения 16.12.2023).

²¹ *Киберпол в Казахстане: борьба с киберпреступностью и ее виды* // <https://toppress.kz/article/kiberpol-v-kazahstane-borba-s-kiberprestupnostyu-i-ee-vidi> (дата обращения 16.12.2023).

государства призывали к разработке нового правового документа о киберпреступности, утверждая, что Будапештская конвенция не предоставляет достаточных возможностей для сотрудничества по этому вопросу. Другие говорили, что укрепление существующих инструментов, включая Конвенцию ООН и Будапештскую конвенцию, было правильным направлением.

С точки зрения аргументов против необходимости начать новый договорный процесс, большинство государств-членов ЕС и ОЭСР поддерживают Будапештскую конвенцию и считают ее прочной основой для глобального документа, утверждая, что она стимулирует многостороннее сотрудничество в борьбе с киберпреступностью и включает в себя много подписавшихся сторон из других регионов мира [14]. Будапештская конвенция является обязательным документом, касающимся трансграничного сотрудничества в области киберпреступности и способствующим гармонизации законов. Многие западные страны считают, что конвенция установила передовой опыт сотрудничества и обеспечивает адекватные гарантии для цифровых прав. Они подчеркивают межрегиональное членство как признак того, что его можно использовать в качестве международной основы [15].

Таким образом, борьба с трансграничными преступлениями, к которым относится и большая часть киберпреступлений, лежит на плечах как отдельных государств, так и мирового сообщества, и только при хорошо скоординированной работе силовых и информационных органов различных стран является возможным снизить количество совершаемых правонарушений в исследуемой сфере.

Проведённое исследование даёт основания утверждать, что для создания условий надлежащей и эффективной деятельности по противодействию киберпреступности недостаточно ресурсов одного правоохранительного органа или правоохранительных органов определённого государства. Такая деятельность должна иметь комплексный характер и предусматривать участие многих стран, что требует необходимого нормативно-правового базиса на глобальном уровне.

Заключение

Одним из решающих факторов в борьбе с киберпреступностью должна стать не только ратификация Будапештской Конвенции отдельными государствами, но и гармонизация национального законодательства с уче-

том основных ее положений, то есть выработка механизмов на национальном уровне. Если национальным законодательством одной из сторон не предусмотрены полномочия искать доказательства в Интернет-среде, то эта сторона не сможет в полном объёме предоставить помощь другой стороне в расследовании киберпреступлений. Таким образом, согласование функций и полномочий между государствами по осуществлению мер по расследованию киберпреступлений является чрезвычайно важным моментом в международной кооперации. Одной из главных причин, из-за которой наблюдается стремительный рост киберпреступности, можно отметить отсутствие единой базы правоохранительных органов, в сферу компетенции которых входит борьба с киберпреступлениями, и ограниченность внутреннего законодательства. Можно констатировать, что важнейшей составляющей стратегии по борьбе с киберпреступностью должно быть всестороннее международное сотрудничество в этой отрасли, поскольку противодействовать киберугрозам на уровне отдельных государств не представляется возможным из-за трансграничной природы данного рода преступлений.

Анализируя стратегии кибербезопасности разных стран, можно выделить объединяющие ключевые позиции, которым необходимо следовать:

- разработка адекватного механизма, позволяющего в общественно-государственном партнерстве, который мог бы позволить и государственным, и частным заинтересованным структурам вырабатывать и утверждать политику борьбы с проблемой киберпреступности;
- детерминация главных целей и путей развития возможностей государства, а также внедрение необходимой нормативной базы для участия в международной борьбе с киберпреступлениями;
- повышение уровня готовности, ускорение реакции на отдельные инциденты, выработка плана восстановления после сбоев и разработка механизмов охраны центральных информационных инфраструктур.

Борьба с киберпреступностью в международном формате актуализирует необходимость координации действий государственного и частного секторов на основе объединения финансовых, технических, коммуникационных и организационных ресурсов, ограничения анонимности пользователей во всемирной сети Интернет,

социальных сетях и во время проведения банковских операций. Также есть потребность в создании международных подразделений и структур для борьбы с киберпреступностью с предоставлением права

передачи данных трафика, экстрадицию, помощь, разработку международных или трансграничных коммуникационных сетей для отслеживания в реальном времени и передачи информации о киберпреступлениях.

ЛИТЕРАТУРА

1. Сералиева А.М. Қазақстан Республикасындағы киберқылмыстың криминологиялық аспектілері // Қазақстан Республикасы ІІМ М. Есболатов ат. Алматы академиясының ғылыми еңбектері. – 2023. - №1(74). – 123 – 133 б.
2. Хусаинов О.Б., Коржумбаева Т.М. Международный опыт правового регулирования противодействия преступности в сфере высоких технологий // Ученые труды Алма-тинской академии МВД Республики Казахстан имени М. Есболатова – 2023. - №1(74). – С. 359-369.
3. Maras M.H. *Cyber criminology*. – Oxford: Oxford University Press, 2017. - 425 p.
4. Данильченко Э.Д. Правовая основа противодействия правоохранительных органов кибертерроризму // Транспортное право. - 2015. - №4. – С. 27-32.
5. Якимова Е.М., Нарутто С.В. Международное сотрудничество в борьбе с киберпреступностью // Криминологический журнал Байкальского государственного университета экономики и права. — 2016. — Т. 10, № 2. — С. 369–378. // <https://cyberleninka.ru/article/n/mezhdunarodnoe-sotrudnichestvo-v-borbe-s-kiberprestupnostyu> (дата обращения 16.12.2023)
6. Smith R.G. (2007). *Crime control in the digital age: An exploration of human rights implications* // *International Journal of Cyber Criminology*. Volume 1(2), pp.167–179 // https://www.researchgate.net/publication/242359325_Crime_Control_in_the_Digital_Age_An_exploration_of_Human_Rights_Implications (дата обращения 16.12.2023)
7. Van der Hof S and Koops B.-J., *Adolescents and Cybercrime: Navigating between Freedom and Control* // *Policy & Internet*. – 2011. -Volume 3 (2), pp. 1-28// https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1868106 (дата обращения 16.12.2023)
8. Карпова Д.Н. Киберпреступность: глобальная проблема и ее решение // Власть. - 2014, № 8. -С. 46-50.
9. McGuire M and Dowling S. *Cyber-crime: A review of the evidence. Chapter 4: Improving the cyber-crime evidence base. Home Office Research Report 75 October 2013* // <https://assets.publishing.service.gov.uk/media/5a7caa0340f0b65b3de0a624/horr75-chap4.pdf> (дата обращения 16.12.2023)
10. Кусайынқызы А. Феминистская криминалистика и киберпреступления // <https://drfl.kz/ru/feminist-forensics-and-cybercrime> (дата обращения 16.12.2023)
11. Приходько Д.В., Белькова А.А. Киберпреступность как глобальная проблема современности // Экономика и бизнес: теория и практика. – 2021. - №4(74). – С.90-94. // <https://cyberleninka.ru/article/n/kiberprestupnost-kak-globalnaya-problema-sovremennosti> (дата обращения 16.12.2023)
12. Право цифровой среды: монография / под ред. Т. П. Подшивалова, Е. В. Титовой, Е. А. Громоной. – Москва: Проспект, 2022. – 896 с. // <http://ivo.garant.ru> (дата обращения 16.12.2023)
13. Kierkegaard S. 2007. *Cybercrime convention: Narrowing the cultural and privacy gap?* // *International Journal of Intercultural Information Management*. – 2007. Volume 1 (1). - 17-32. // https://www.researchgate.net/publication/228149657_Cybercrime_Convention_Narrowing_the_Cultural_and_Privacy_Gap (дата обращения 16.12.2023)
14. Kavanagh C. *The United Nations, cyberspace and international peace and security: Responding to complexity in the 21st century*. Geneva: United Nations Institute for Disarmament Research // <https://unidir.org/files/publication/pdfs/the-united-nations-cyberspace-and-international-peace-and-security-en-691.pdf> (дата обращения 16.12.2023)
15. Shore M., Du. Yi, and Zeadally S. *A public-private partnership model for national cyber security* // *Policy & Internet*. - 2011. - Volume 3 pp. 1–23. https://www.researchgate.net/publication/261543516_A_Public-Private_Partnership_Model_for_National_Cybersecurity (дата обращения 16.12.2023)

REFERENCES

1. Seralieva A.M. *Qazaqstan Respublikasyndaғы kiberqylmystың kriminologijalyқ aspektileri* // *Qazaqstan Respublikasy IIM M. Esbolatov at. Almaty akademijasynың ғылыми еңбектері.* – 2023. - №1(74). – 123 – 133 b.
2. Husainov O.B., Korzhumbaeva T.M. *Mezhdunarodnyj opyt pravovogo regulirovaniya protivodejstviya prestupnosti v sfere vysokih tehnologij* // *Uchenye trudy Almatinskoj akademii MVD Respubliki Kazahstan imeni M. Esbolatova* – 2023. - №1(74). – S. 359-369.
3. Maras M.H. *Cyber criminology.* – Oxford: Oxford University Press, 2017. - 425 r.
4. Danil'chenko Je.D. *Pravovaja osnova protivodejstviya pravoohranitel'nyh organov kiberterrorizmu* // *Transportnoe pravo.* - 2015. - №4. – S. 27-32.
5. Jakimova E.M., Narutto S.V. *Mezhdunarodnoe sotrudnichestvo v bor'be s kiberprestupnost'ju* // *Kriminologicheskij zhurnal Bajkal'skogo gosudarstvennogo universiteta jekonomiki i prava.* — 2016. — T. 10, № 2. — S. 369–378. // <https://cyberleninka.ru/article/n/mezhdunarodnoe-sotrudnichestvo-v-borbe-s-kiberprestupnostyu> (data obrashhenija 16.12.2023)
6. Smith R.G. (2007). *Crime control in the digital age: An exploration of human rights implications* // *International Journal of Cyber Criminology. Volume 1(2), rr.167–179* // https://www.researchgate.net/publication/242359325_Crime_Control_in_the_Digital_Age_An_exploration_of_Human_Rights_Implications (data obrashhenija 16.12.2023)
7. Van der HofS and Koops B.-J., *Adolescents and Cybercrime: Navigating between Freedom and Control* // *Policy & Internet.* – 2011. -Volume 3 (2), rr. 1-28// https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1868106 (data obrashhenija 16.12.2023)
8. Karpova D.N. *Kiberprestupnost': global'naja problema i ee reshenie* // *Vlast'.* - 2014, № 8. -S. 46-50.
9. McGuireM and Dowling S. *Cyber-crime: A review of the evidence. Chapter 4: Improving the cyber-crime evidence base. Home Office Research Report 75 October 2013* // <https://assets.publishing.service.gov.uk/media/5a7caa0340f0b65b3de0a624/horr75-chap4.pdf> (data obrashhenija 16.12.2023)
10. Kusajynkyzy A. *Feministskaja kriminalistika i kiberprestuplenija* // <https://drfl.kz/ru/feminist-forensics-and-cybercrime> (data obrashhenija 16.12.2023)
11. Prihod'ko D.V., Bel'kova A.A. *Kiberprestupnost' kak global'naja problema sovremennosti* // *Jekonomika i biznes: teorija i praktika.* – 2021. - №4(74). – S.90-94. // <https://cyberleninka.ru/article/n/kiberprestupnost-kak-globalnaya-problema-sovremennosti> (data obrashhenija 16.12.2023)
12. *Pravo cifrovoj sredy: monografija / pod red. T. P. Podshivalova, E. V. Titovoj, E. A. Gromovoj.* – Moskva: Prospekt, 2022. – 896 s. // <http://ivo.garant.ru> (data obrashhenija 16.12.2023)
13. Kierkegaard S. 2007. *Cybercrime convention: Narrowing the cultural and privacy gap?* // *International Journal of Intercultural Information Management.* – 2007. Volume 1 (1). - 17-32. // https://www.researchgate.net/publication/228149657_Cybercrime_Convention_Narrowing_the_Cultural_and_Privacy_Gap (data obrashhenija 16.12.2023)
14. Kavanagh C. *The United Nations, cyberspace and international peace and security: Responding to complexity in the 21st century.* Geneva: United Nations Institute for Disarmament Research // <https://unidir.org/files/publication/pdfs/the-united-nations-cyberspace-and-international-peace-and-security-en-691.pdf> (data obrashhenija 16.12.2023)
15. Shore M., Du. Yi, and Zeadally S. *A public-private partnership model for national cyber security* // *Policy & Internet.* - 2011. - Volume3 rr. 1–23. https://www.researchgate.net/publication/261543516_A_Public-Private_Partnership_Model_for_National_Cybersecurity (data obrashhenija 16.12.2023)