МРНТИ 10.91.91
УДК 343.9:004.738.5(574)
JEL K24

https://doi.org/10.46914/2959-4197-2026-1-2-317-328

ЖАНДЫКЕЕВА Г.Е.,*[1]
PhD, ст. преподаватель.
*e-mail: zhagulnar@gmail.com
ORCID ID: 0000-0003-3736-5292
ТОРГАУТОВА Б.А.,[2]
к.ю.н., доцент.
b.torgautova@etu.edu.kz
ORCID ID: 0000-0002-8793-3297
ЖАНДЫКЕЕВА А.К.,[3]
магистр права.
e-mail: Azhandykeyeva@gmail.com
ORCID ID: 0009-0004-5497-1512
КУНДАКОВА М.Ж.,[4]
PhD, ассоциированный профессор.
e-mail: kundakovam@gmail.com
ORCID ID: 0009-0008-9846-4503
[1]Q University,
г. Алматы, Казахстан
[2]META University,
г. Алматы, Казахстан
[3]ТОО «Многопрофильный
инновационный колледж»,
г. Алматы, Казахстан
[4]ALT университет,
г. Алматы, Казахстан

ИМПЛЕМЕНТАЦИЯ МЕЖДУНАРОДНЫХ СТАНДАРТОВ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ В УГОЛОВНОМ ЗАКОНОДАТЕЛЬСТВЕ КАЗАХСТАНА

Аннотация

В статье рассматриваются теоретические и практические вопросы имплементации международных стандартов противодействия киберпреступности в уголовное законодательство Республики Казахстан. Проведен сравнительно-правовой анализ положений Конвенции ООН против киберпреступности (ред. 2024 г.) и норм Уголовного и Уголовно-процессуального кодексов Республики Казахстан (ред. 2025 г.). Определены пробелы и несоответствия, препятствующие эффективному применению уголовно-правовых норм в условиях цифровизации. Выявлено, что казахстанское законодательство лишь частично охватывает составы преступлений, связанных с незаконным перехватом данных, вмешательством в функционирование информационных систем и иными формами цифровых правонарушений. Обоснована необходимость внедрения самостоятельных составов преступлений, корреспондирующих статьям 8–17 и 23–35 Конвенции ООН, а также совершенствования процессуальных механизмов международного сотрудничества и обращения с электронными доказательствами. Сделан вывод о том, что гармонизация национального законодательства с международными нормами является важным условием укрепления цифровой безопасности и повышения эффективности уголовного правосудия в Республике Казахстан.

Ключевые слова: киберпреступность, законодательство, конвенция, имплементация, безопасность, электронные доказательства.

Введение

В эпоху стремительного развития информационно-телекоммуникационных технологий и цифровой трансформации [1] всех сфер общественной жизни вопрос противодействия киберпреступности выходит на передний план в сфере уголовного процесса, криминалистики и судебной экспертизы. Современное общество сталкивается с тем, что преступления в киберпространстве – от несанкционированного доступа к данным до международных мошеннических схем и распространения детской порнографии через цифровые сети – приобретают трансграничный характер, высокую технологическую сложностью и требуют специальной правовой и организационной реакции. В данном контексте для Республики Казахстан становится важной задачей адекватное правовое регулирование, которое не только учитывает национальные особенности, но и соответствует международным стандартам.

Актуальность темы обусловлена тем, что обладание современной уголовно-правовой базой в области киберпреступности является одним из критериев правовой безопасности государства, надежности функционирования цифровой экономики и защиты прав и свобод граждан.

Развитие цифровой инфраструктуры Республики Казахстан сопровождается активным внедрением электронного правительства, цифровых банковских сервисов, платформ дистанционного взаимодействия и облачных технологий хранения данных. Существенная часть государственных и частных услуг уже переведена в электронный формат, что объективно увеличивает объем информации, циркулирующей в цифровой среде. Одновременно возрастает и количество угроз, связанных с несанкционированным доступом к данным, вмешательством в функционирование информационных систем, цифровым мошенничеством и незаконным использованием персональной информации. В условиях высокой зависимости государства, финансового сектора и граждан от устойчивости информационно-коммуникационных систем вопросы уголовно-правовой защиты цифрового пространства приобретают стратегическое значение и требуют постоянного совершенствования национального законодательства.

Тем не менее, несмотря на усилия казахстанского законодателя и правоохранительной практики, просматриваются заметные разрывы между требованиями международных соглашений и национальным уголовным законодательством.

Согласно материалам Конвенции Совета Европы о киберпреступности (Будапештская конвенция) [2] и Конвенции ООН против киберпреступности [3], мировое сообщество закрепляет целый ряд новых составов преступлений, специальных мер по сбору и передаче электронных доказательств, а также механизмов международного сотрудничества и ответственности юридических лиц. На уровне Уголовного кодекса Республики Казахстан [4] (далее – УК Республики Казахстан) и сопутствующих нормативных актов часть таких положений отсутствует либо имплементирована фрагментарно. Так, Казахстан на 19 апреля 2023 г. был приглашен к присоединению к Будапештской конвенции, став наблюдателем в Комитете по киберпреступности [5].

Особенность киберпреступности заключается в ее выраженном трансграничном характере. Значительная часть противоправных действий совершается с использованием серверов, облачных платформ и цифровых сервисов, расположенных за пределами государства, в котором наступают общественно опасные последствия. В подобных условиях применение исключительно национальных механизмов уголовного преследования оказывается недостаточным. Эффективное расследование цифровых преступлений требует унификации уголовно-правовых подходов, согласования процедур обращения с электронными доказательствами и формирования устойчивых механизмов международного сотрудничества между правоохранительными органами различных государств. Именно поэтому международные конвенции в сфере противодействия киберпреступности постепенно становятся универсальным ориентиром для модернизации национального законодательства.

В научной литературе обращается внимание на наличие значительных расхождений между положениями международных конвенций в сфере противодействия киберпреступности и национальным уголовным законодательством Республики Казахстан. Так, исследователи указывают на «нестыковки между национальным законодательством Республики Казахстан и положениями Конвенции» в части определения состава киберпреступлений, порядка изъятия и сохранения электронных доказательств, а также механизмов международного взаимодействия правоохранительных органов [6, 7, 8].

Таким образом, возникает проблемное поле: как обеспечить эффективную имплементацию международных стандартов в уголовно-правовую систему Казахстана, чтобы устранить нормативные пробелы, повысить качество расследований и судебных решений и одновременно обеспечить защиту прав и свобод граждан в цифровой среде.

Целью настоящей статьи является проведение сравнительно-правового анализа международных стандартов противодействия киберпреступности, в частности положений Конвенции ООН и релевантных международных договоров и уголовного законодательства Республики Казахстан с выявлением нормативных пробелов, оценкой их влияния на практику уголовного преследования в сфере киберпреступлений и формулировкой рекомендаций по совершенствованию национальной правовой базы. В процессе исследования предполагается установить, какие именно положения международного права еще не интегрированы в УК Республики Казахстан, какие последствия это порождает в уголовно-правовом поле и какие шаги необходимо предпринять для их полноценной имплементации в интересах повышения эффективности борьбы с киберпреступностью.

Материалы и методы

Исследование выполнено в рамках сравнительно-правового анализа с элементами контент-анализа нормативных правовых актов и официальной статистики. Дизайн исследования имеет аналитико-дескриптивный характер и направлен на выявление соответствий и расхождений между международными стандартами противодействия киберпреступности, закрепленными в Конвенции ООН против киберпреступности, и положениями Уголовного законодательства Республики Казахстан в редакции 2025 г. Основное внимание уделено нормативным, содержательным и институциональным аспектам правового регулирования в сфере кибербезопасности.

В качестве материала для анализа использовались официальные тексты международных договоров, национальных законодательных актов, а также научные труды отечественных и зарубежных исследователей, опубликованные в рецензируемых правовых изданиях.

Методологическую основу составили общенаучные методы анализа, синтеза, индукции и дедукции, а также специальные методы сравнительного правоведения, формально-юридического и системно-структурного анализа.

Применение сравнительно-правового метода позволило определить степень соответствия уголовного законодательства Республики Казахстан положениям международных договоров в сфере противодействия киберпреступности. Использование формально-юридического анализа обеспечило возможность выявления нормативных пробелов и коллизий, возникающих при регулировании цифровых правонарушений. Дополнительно использовались элементы статистического анализа официальных данных Министерства внутренних дел и Генеральной прокуратуры Республики Казахстан, что позволило сопоставить состояние правового регулирования с фактической динамикой роста киберпреступности. Системный подход обеспечил рассмотрение вопросов цифровой безопасности не только с позиции уголовного права, но и в контексте международного сотрудничества, деятельности правоохранительных органов и развития информационно-коммуникационных технологий.

Дополнительно сравнительный анализ проводился по направлениям, отражающим ключевые области регулирования, предусмотренные Конвенцией ООН против киберпреступности и соответствующими разделами уголовного законодательства Республики Казахстан. Для каждого направления оценивались наличие аналогичных норм в национальном праве, степень соответствия международным стандартам, а также эффективность практического применения.

Результаты

Проведенный сравнительно-правовой анализ показал, что действующее уголовное законодательство Республики Казахстан лишь частично соответствует международным стандартам противодействия киберпреступности, закрепленным в Конвенции ООН против киберпреступности и Будапештской конвенции. Наиболее существенные пробелы выявлены в части криминализации незаконного перехвата данных, регулирования вмешательства в функционирование

информационных систем, обращения с электронными доказательствами и установления ответственности юридических лиц.

Анализ также показал, что отдельные нормы главы 7 УК Республики Казахстан не учитывают современные формы цифровых преступлений, совершаемых с использованием распределенных сетей, вредоносного программного обеспечения и трансграничных цифровых платформ.

В качестве эмпирической базы использованы официальные данные МВД о зарегистрированных преступлениях, совершенных с использованием ИКТ. Так, по данным МВД, в 2024 г. зарегистрировано свыше 17 000 случаев интернет-мошенничества [9]. При этом раскрыто лишь около 20 % таких дел – из 15 905 дел раскрыто 3 286 [10].

Из анализа также видно, что за последние пять лет количество киберпреступлений выросло почти в три раза, где почти половина всех уголовных правонарушений по статье «Мошенничество» относится к интернет-мошенничеству (48,6 %) [11].

Такая динамика подтверждает необходимость гармонизации уголовного законодательства с международными нормами и разработки специализированных составов, отражающих специфику цифровых преступлений.

Сфера уголовно-правового регулирования киберпреступлений в Конвенции и УК Республики Казахстан

Конвенция ООН против киберпреступности, принятая резолюцией Генеральной Ассамблеи ООН 24 декабря 2024 г. (далее – Конвенция), определяет киберпреступность как использование ИКТ в преступных целях и устанавливает минимальные стандарты уголовной ответственности за такие деяния.

Документ выделяет четыре ключевые группы преступлений:

1. Преступления против конфиденциальности, целостности и доступности данных и систем (ст. 8–10).

2. Компьютерное мошенничество и подделка данных (ст. 11–13).

3. Преступления, связанные с контентом (ст. 14).

4. Сопутствующие преступления, включая отмывание доходов, пособничество, соучастие и ответственность юридических лиц (ст. 15–17).

В свою очередь, УК Республики Казахстан содержит лишь общие нормы, применяемые к информационным технологиям, а именно:

ст. 205 – Неправомерный доступ к информации;

ст. 206 – Неправомерные уничтожение или модификация информации;

ст. 207 – Нарушение работы объекта информатизации;

ст. 208 – Неправомерное завладение информацией;

ст. 209 – Принуждение к передаче информации;

ст. 210 – Создание, использование или распространение вредоносных компьютерных программ и программных продуктов;

ст. 211 – Неправомерное распространение электронных информационных ресурсов ограниченного доступа;

ст. 212 – Предоставление услуг для размещения интернет-ресурсов, преследующих противоправные цели;

ст. 213 – Неправомерные изменение идентификационного кода абонентского устройства сотовой связи, устройства идентификации абонента, а также создание, использование, распространение программ для изменения идентификационного кода абонентского устройства;

п.4 ч.2 ст. 190 – Мошенничество, совершенное путем обмана или злоупотребления доверием пользователя информационной системы или сети Интернет;

ст. 312 – Изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних либо их привлечение для участия в зрелищных мероприятиях порнографического характера.

Однако анализ показывает, что данные нормы не охватывают весь спектр составов, предусмотренных международными стандартами.

Во-первых, незаконный перехват данных ст. 8 Конвенции требует криминализации умышленного перехвата данных в процессе их передачи (например, через сетевые протоколы или

беспроводные каналы). В УК Республики Казахстан аналогичной нормы нет. Статья 147 «Нарушение неприкосновенности частной жизни» и статья 205 частично охватывают вмешательство в частную информацию, но не предусматривают ответственности за сам факт перехвата, без доступа к содержимому.

Тем самым авторами рекомендуется ввести отдельную статью «Незаконный перехват электронных данных», установив ответственность за перехват трафика или сообщений без разрешения владельца.

Во-вторых, вмешательство в данные и системы ст. 9–10 Конвенции предусматривает ответственность за удаление, изменение, блокирование или разрушение электронных данных и нарушение функционирования систем. В УК Республики Казахстан нет прямого аналога. Статья 205 ограничивается лишь фактом доступа без разрешения.

Практический пример: техническими подразделениями Комитета национальной безопасности Республики Казахстан отражены 86,3 млн кибератак и 2156 DDoS-атак на ресурсы госорганов и стратегические объекты в 2023 г. [12].

Авторы также рекомендуют дополнить УК Республики Казахстан статьей «Вмешательство в функционирование информационно-коммуникационных систем», аналогичной статье 5 Будапештской конвенции.

В-третьих, ответственность юридических лиц ст. 16 Конвенции прямо указывает на необходимость установления уголовной или административной ответственности юридических лиц за киберпреступления. УК Республики Казахстан такую возможность не предусматривает, ограничиваясь привлечением должностных лиц.

Авторы рекомендуют внести изменения в Общую часть УК, установив ответственность юридических лиц за киберпреступления, совершенные в их интересах или при их содействии.

В-четвертых, международное сотрудничество и электронные доказательства, в главе IV Конвенции закреплен принцип немедленного обмена информацией и оперативного сохранения электронных доказательств (ст. 23–35). Уголовно-процессуальное законодательство Казахстана (далее – УПК Республики Казахстан) таких механизмов не содержит.

По данным Генеральной прокуратуры Республики Казахстан, в первом полугодии 2024 г. зарегистрировано 22 600 уголовных правонарушений в сфере интернет-мошенничества, что на 10,4% больше, чем за аналогичный период 2023 г. [13].

Авторами рекомендуется разработать в УПК Республики Казахстан специальные нормы о сохранении и передаче электронных доказательств, а также создать национальную контактную точку 24/7, как это предусмотрено Конвенцией.

Таблица 1 – Результаты сравнительного анализа

Направление	Конвенция ООН	УК, УПК РК	Уровень соответствия
Незаконный перехват данных	Ст. 8	Нет аналога	Низкий
Вмешательство в данные и системы	Ст. 9–10	Частично (ст. 205, 206)	Средний
Ответственность юрлиц	Ст. 16	Отсутствует	Низкий
Электронные доказательства, международное сотрудничество	Ст. 23–35	Не урегулировано	Низкий
Примечание: Составлено авторами на основе Конвенции ООН против киберпреступности, Будапештской конвенции и Уголовного кодекса Республики Казахстан.			

Полученные результаты сравнительного анализа свидетельствуют о том, что наибольшие сложности возникают именно в сфере квалификации преступлений, связанных с незаконным перехватом цифровой информации и вмешательством в функционирование информационных систем. Отсутствие самостоятельного уголовно-правового состава, предусматривающего ответственность за перехват сетевого трафика и непубличной передачи данных, существенно ос-

ложняет практику расследования преступлений, совершаемых с использованием вредоносного программного обеспечения, фишинговых платформ и средств скрытого мониторинга пользовательской активности. На практике подобные действия нередко квалифицируются по смежным составам, что приводит к размытости правовой оценки и затрудняет формирование единообразной судебной практики.

Отдельной проблемой остается обращение с электронными доказательствами. Цифровая информация обладает высокой степенью изменяемости и может быть удалена либо модифицирована за короткий промежуток времени. Дополнительные сложности возникают в ситуациях, когда сведения размещены на зарубежных серверах или распределены между несколькими облачными хранилищами, находящимися под юрисдикцией различных государств. Отсутствие в уголовно-процессуальном законодательстве Республики Казахстан процедур оперативного сохранения электронных данных и ускоренного международного взаимодействия снижает эффективность расследования и повышает риск утраты доказательственной базы.

Не менее значимым остается вопрос ответственности юридических лиц. Современные киберпреступления нередко совершаются с использованием инфраструктуры коммерческих организаций, хостинг-платформ, анонимных сервисов и цифровых посредников, обеспечивающих хранение либо передачу информации. Международные стандарты постепенно переходят к модели, при которой юридическое лицо может нести самостоятельную ответственность за создание условий для совершения киберпреступлений или получение выгоды от противоправной цифровой деятельности. В уголовном законодательстве Республики Казахстан подобный механизм пока отсутствует, что ограничивает возможности комплексного противодействия организованной киберпреступности.

Обсуждение

Результаты анализа показывают, что казахстанское уголовное законодательство находится на стадии адаптации к международным стандартам. Большинство норм УК Республики Казахстан охватывают лишь отдельные аспекты киберпреступности, не создавая целостной системы регулирования. Главной проблемой остается устаревшая структура состава преступлений, ориентированная на материальные объекты, тогда как киберпреступления совершаются в нематериальной цифровой среде.

Аналогичные тенденции наблюдаются и в зарубежной практике. В государствах Европейского союза имплементация положений Будапештской конвенции сопровождалась созданием специализированных подразделений цифровой криминалистики, внедрением процедур срочного сохранения электронных доказательств и расширением международного обмена информацией между правоохранительными органами. В США соответствующие механизмы реализуются в рамках Computer Fraud and Abuse Act, предусматривающего самостоятельную уголовную ответственность за вмешательство в работу компьютерных систем и незаконный доступ к цифровым данным [14, 15].

Международный опыт показывает, что эффективность противодействия киберпреступности напрямую зависит от скорости обмена цифровыми доказательствами, уровня международной координации и наличия специализированных уголовно-правовых составов, ориентированных именно на цифровую среду [16, 17].

Кроме того, отсутствие института уголовной ответственности юридических лиц, процедур международного обмена доказательствами и правовых основ для срочного «замораживания» электронных данных снижает эффективность расследований и приводит к утрате доказательственной базы.

Обобщенные результаты исследования показывают, что действующие нормы главы 7 УК Республики Казахстан «Уголовные правонарушения в сфере информатизации и связи» требуют пересмотра и дополнения.

В целях имплементации международных стандартов представляется целесообразным дополнить главу 7 УК Республики Казахстан рядом самостоятельных составов уголовных правонарушений.

Во-первых, предлагается предусмотреть статью «Незаконный перехват электронных данных», устанавливающую ответственность за умышленный перехват непубличной передачи компьютерных данных, включая сетевой трафик и электромагнитные сигналы.

Во-вторых, целесообразно закрепить состав «Вмешательство в функционирование информационно-коммуникационных систем», предусматривающий ответственность за блокирование, нарушение либо дестабилизацию работы цифровых систем, включая DDoS-атаки.

В-третьих, требуется криминализация незаконного использования цифровых идентификаторов, электронных ключей и средств аутентификации.

Дополнительно предлагается установить ответственность за незаконный оборот вредоносных цифровых инструментов, включая распространение программного обеспечения, предназначенного для совершения киберпреступлений.

Отдельного правового регулирования требует порядок обращения с электронными доказательствами, включая ответственность за их уничтожение, сокрытие или модификацию в ходе уголовного судопроизводства.

Целесообразно модернизировать данный раздел Особенной части, обеспечив его соответствие положениям статей 8-14 Будапештской конвенции, а также современным тенденциям в сфере ИКТ. Речь идет не о создании новой главы, а об актуализации действующих составов и введении недостающих, отражающих новые формы киберпреступности.

Зарубежный опыт имплементации международных стандартов противодействия киберпреступности.

В зарубежной правоприменительной практике имплементация международных стандартов противодействия киберпреступности осуществляется значительно более системно. Государства Европейского союза адаптировали национальное законодательство в соответствии с положениями Будапештской конвенции, закрепив самостоятельные составы преступлений, связанные с незаконным вмешательством в информационные системы, распространением вредоносного программного обеспечения и незаконным оборотом цифровых данных.

В Германии и Франции особое внимание уделяется процедурам сохранения электронных доказательств и механизмам взаимодействия между интернет-провайдерами и правоохранительными органами. В США действует комплекс федеральных норм, регулирующих расследование компьютерных преступлений и международное сотрудничество в цифровой сфере [18, 19].

В Сингапуре и Южной Корее реализованы специализированные государственные программы кибербезопасности, предусматривающие постоянный мониторинг цифровых угроз, деятельность национальных центров реагирования и ускоренные процедуры обмена электронными доказательствами [18,19].

Дополнительный интерес представляет практика Европейского союза, где противодействие киберпреступности строится на принципе постоянного межгосударственного взаимодействия. Значительную роль играет деятельность Europol и специализированной платформы Joint Cybercrime Action Taskforce, обеспечивающей координацию расследований, обмен оперативной информацией и проведение совместных цифровых операций. В государствах ЕС активно развиваются подразделения цифровой криминалистики, специализирующиеся на анализе электронных доказательств, восстановлении удаленной информации и выявлении трансграничных цифровых связей между участниками преступной деятельности.

В Соединенных Штатах Америки особое внимание уделяется взаимодействию правоохранительных органов с частным сектором. Расследование компьютерных преступлений осуществляется при активном участии интернет-провайдеров, банковских структур и технологических компаний, обладающих доступом к информации о сетевой активности пользователей. Существенное значение имеет возможность экстренного сохранения цифровых данных до получения судебного разрешения, что позволяет минимизировать риск уничтожения электронных доказательств.

Практика государств Восточной Азии также демонстрирует высокий уровень институциональной адаптации к цифровым угрозам. В Южной Корее и Сингапуре функционируют национальные центры реагирования на киберинциденты, осуществляющие постоянный мониторинг сетевой активности, выявление вредоносных цифровых операций и координацию действий

между государственными структурами и частными организациями. Подобный подход позволяет существенно сократить время реагирования на кибератаки и повысить эффективность предотвращения цифровых преступлений [18, 19].

Анализ зарубежного опыта показывает, что современная модель противодействия киберпреступности требует комплексного сочетания уголовно-правовых, процессуальных и организационных механизмов [20].

Отдельного внимания требует влияние технологий искусственного интеллекта на развитие современной киберпреступности. Использование алгоритмов машинного обучения позволяет злоумышленникам автоматизировать фишинговые атаки, создавать реалистичные поддельные цифровые изображения и голосовые сообщения, а также генерировать вредоносный программный код с высокой степенью адаптации к системам защиты. Распространение технологий deepfake дополнительно осложняет вопросы идентификации личности и достоверности электронных доказательств в уголовном судопроизводстве. В связи с этим дальнейшее совершенствование уголовного законодательства должно учитывать не только существующие формы цифровых преступлений, но и потенциальные риски, связанные с применением искусственного интеллекта в противоправной деятельности.

Заключение

Проведенное исследование показывает, что уголовное законодательство Казахстана в сфере противодействия киберпреступности находится в стадии адаптации к международным стандартам. Несмотря на наличие отдельных норм, регулирующих ответственность за преступления в сфере информационных технологий, законодательная база пока не обеспечивает комплексной защиты от угроз цифрового характера.

Основные пробелы связаны с отсутствием в уголовном праве Казахстана самостоятельных составов, отражающих незаконный перехват данных, вмешательство в работу информационных систем, цифровую подделку, а также с отсутствием института уголовной ответственности юридических лиц. Не менее актуальна проблема правового регулирования обращения с электронными доказательствами и механизмов международного обмена данными в режиме «24/7», предусмотренного Конвенцией ООН против киберпреступности.

Реализация предложенных мер, включая обновление главы 7 УК Республики Казахстан, внедрение новых составов преступлений, формализация процедур взаимодействия с иностранными юрисдикциями и создание национального центра быстрого реагирования позволит Казахстану укрепить позиции в сфере цифровой безопасности, повысить раскрываемость киберпреступлений и интегрировать национальную правовую систему в международное пространство правосудия. Гармонизация уголовного законодательства с международными стандартами должна рассматриваться не просто как юридическая реформа, а как стратегическое направление защиты прав граждан и интересов государства в условиях глобальной цифровой трансформации.

Проведенный сравнительно-правовой анализ также показал, что дальнейшее развитие уголовного законодательства Республики Казахстан в сфере цифровой безопасности должно сопровождаться не только обновлением отдельных уголовно-правовых норм, но и формированием единого механизма взаимодействия между следственными органами, судами, экспертными подразделениями и международными организациями.

Практическая реализация предложенных изменений позволит повысить эффективность расследования киберпреступлений, сократить уровень латентности цифровых правонарушений и обеспечить более устойчивую защиту информационной инфраструктуры государства. Особое значение данные меры приобретают в условиях роста трансграничной цифровой преступности и расширения применения искусственного интеллекта в противоправной деятельности.

Современные тенденции цифровизации показывают, что развитие информационно-коммуникационных технологий неизбежно сопровождается усложнением способов совершения преступлений в виртуальной среде. В подобных условиях уголовное законодательство должно развиваться опережающими темпами, обеспечивая своевременную адаптацию правовых меха-

низмов к новым цифровым угрозам. Нормативное отставание в сфере регулирования киберпреступности способно привести к снижению эффективности уголовного преследования, росту латентности цифровых правонарушений и ослаблению доверия к системе государственной защиты информации. По этой причине имплементация международных стандартов должна рассматриваться как долгосрочное стратегическое направление модернизации уголовно-правовой политики Республики Казахстан.

Полученные результаты могут быть использованы при дальнейшем совершенствовании уголовного и уголовно-процессуального законодательства Республики Казахстан, а также при разработке национальных программ цифровой безопасности и подготовки специалистов в сфере расследования киберпреступлений.

ЛИТЕРАТУРА

1 Постановление Правительства Республики Казахстан № 269 «Об утверждении Концепции цифровой трансформации, развития отрасли информационно-коммуникационных технологий и кибербезопасности на 2023-2029 годы» от 28 марта 2023 года. URL: https://adilet.zan.kz/rus/docs/P2300000269 (дата обращения: 08.05.2026)

2 Совет Европы. Конвенция Совета Европы о противодействии киберпреступлениям, Будапешт, 23.11.2001. URL: https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf (дата обращения: 08.05.2026)

3 Указ Президента Республики Казахстан № 1067 «О подписании Конвенции Организации Объединенных Наций против киберпреступности; укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям» от 24 октября 2025 года. URL: https://adilet.zan.kz/rus/docs/U2500001067#z9 (дата обращения: 08.05.2026)

4 Уголовный кодекс Республики Казахстан № 226-V ЗРК от 3 июля 2014 года. URL: https://adilet.zan.kz/rus/docs/K1400000226 (дата обращения: 08.05.2026)

5 Проект «Осьминог»: власти Казахстана координируют дальнейшие шаги для завершения присоединения к Конвенции о киберпреступности. Астана, Казахстан 13–14 ноября 2024 г. URL: https://www.coe.int/en/web/cybercrime/-/octopus-project-authorities-of-kazakhstan-coordinate-on-the-next-steps-to-complete-accession-to-the-convention-on-cybercrime (дата обращения: 08.05.2026)

6 Сатбаева А.М. Проблемы противодействия киберпреступности: опыт международного сотрудничества // Вестник Института законодательства и правовой информации Республики Казахстан. – 2024. – № 3(78). – С. 211–221. DOI: 10.52026/2788-5291-2024-78-3-211

7 Apsimet N.M., Muratova A.Zh. On the possibility of using the provisions of the Budapest Convention on cybercrime in the investigation of crimes in the field of online fraud. Law Series. Bulletin of Karaganda University. 2025. V. 30. No. 1(117). P. 87–97. DOI: 10.31489/2025L1/87-97

8 Мырзаханова А.К., Абайдельданов Е.М. Имплементация норм международного права в национальное законодательство Республики Казахстан. BULLETIN of L.N. Gumilyov Eurasian National University // LAW Series. – 2019. – № 2 – С. 113–123. DOI: 10.32523/2616-6844-2019-127-2-113-123

9 В 2024-м зарегистрировано более 17 тыс. случаев интернет-мошенничества // Казахстанская правда. URL: https://kazpravda.kz/n/v-2024-m-zaregistrirovano-bolee-17-tys-sluchaev-internet-moshennichestva/ (дата обращения: 08.05.2026)

10 В Казахстане раскрывается лишь пятая доля интернет-преступлений // PROFIT Online. URL: https://profit.kz/news/68399/V-Kazahstane-raskrivaetsya-lish-pyataya-dolya-internet-prestuplenij (дата обращения: 08.05.2026)

11 Число киберпреступлений в Казахстане за 5 лет выросло почти в три раза // Atameken Business. URL: https://www.inbusiness.kz/ru/last/chislo-kiberprestuplenij-v-kazahstane-za-5-let-vyroslo-pochti-v-tri-raza (дата обращения: 08.05.2026)

12 Кескин О. В Казахстане в 2023 году отразили 86,3 млн кибератак на ресурсы госорганов и важные объекты. 2024. URL: https://clck.su/obTbv (дата обращения: 08.05.2026)

13 Генеральная прокуратура подвела итоги работы за первое полугодие 2024 года // Единая платформа интернет-ресурсов государственных органов. URL: https://kazpravda.kz/n/generalnaya-prokuratura-podvela-itogi-raboty-za-pervoe-polugodie-2024-goda/ (дата обращения: 08.05.2026)

14 Brenner S.W. Cybercrime and the Law. Boston: Northeastern University Press, 2022. 412 p.

15 Clough J. Principles of Cybercrime. Cambridge: Cambridge University Press, 2021. 598 p.

16 Wall D. Cybercrime and Society. London: Sage Publications, 2023. 287 p.

17 Broadhurst R., Grabosky P. Cybercrime in Asia. Singapore: Springer, 2021. 355 p.

18 UNODC. Comprehensive Study on Cybercrime. Vienna: United Nations Office on Drugs and Crime, 2024. 320 p.

19 Europol. Internet Organised Crime Threat Assessment 2024. URL: https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024 (accessed: 08.05.2026)

20 Gordon S., Ford R. On the Definition and Classification of Cybercrime // Journal in Computer Virology. 2022. Vol. 18. No. 2. P. 145–159.

REFERENCES

1 Postanovlenie Pravitel'stva Respubliki Kazahstan No. 269 «Ob utverzhdenii Koncepcii cifrovoj transformacii, razvitija otrasli informacionno-kommunikacionnyh tehnologij i kiberbezopasnosti na 2023-2029 gody» ot 28 marta 2023 goda. URL: https://adilet.zan.kz/rus/docs/P2300000269 (data obrashhenija: 08.05.2026). (In Russian)

2 Sovet Evropy. Konvencija Soveta Evropy o protivodejstvii kiberprestuplenijam, Budapesht, 23.11.2001. URL: https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf (data obrashhenija: 08.05.2026). (In Russian)

3 Ukaz Prezidenta Respubliki Kazahstan No. 1067 «O podpisanii Konvencii Organizacii Ob#edinennyh Nacij protiv kiberprestupnosti; ukreplenie mezhdunarodnogo sotrudnichestva v bor'be s opredelennymi prestuplenijami, sovershaemymi s ispol'zovaniem informacionno-kommunikacionnyh sistem, i v obmene dokazatel'stvami v jelektronnoj forme, otnosjashhimisja k ser'eznym prestuplenijam» ot 24 oktjabrja 2025 goda. URL: https://adilet.zan.kz/rus/docs/U2500001067#z9 (data obrashhenija: 08.05.2026). (In Russian)

4 Ugolovnyj kodeks Respubliki Kazahstan No. 226-V ZRK ot 3 ijulja 2014 goda. URL: https://adilet.zan.kz/rus/docs/K1400000226 (data obrashhenija: 08.05.2026). (In Russian)

5 Proekt «Os'minog»: vlasti Kazahstana koordinirujut dal'nejshie shagi dlja zavershenija prisoedinenija k Konvencii o kiberprestupnosti. Astana, Kazahstan 13–14 nojabrja 2024 g. URL: https://www.coe.int/en/web/cybercrime/-/octopus-project-authorities-of-kazakhstan-coordinate-on-the-next-steps-to-complete-accession-to-the-convention-on-cybercrime (data obrashhenija: 08.05.2026). (In Russian)

6 Satbaeva A.M. (2024) Problemy protivodejstvija kiberprestupnosti: opyt mezhdunarodnogo sotrudnichestva // Vestnik Instituta zakonodatel'stva i pravovoj informacii Respubliki Kazahstan. No. 3(78). P. 211–221. DOI: 10.52026/2788-5291-2024-78-3-211 (In English)

7 Apsimet N.M., Muratova A.Zh. (2025) On the possibility of using the provisions of the Budapest Convention on cybercrime in the investigation of crimes in the field of online fraud. Law Series. Bulletin of Karaganda University. V. 30. No. 1(117). P. 87–97. DOI: 10.31489/2025L1/87-97 (In English)

8 Myrzahanova A.K., Abajdel'danov E.M. (2019) Implementacija norm mezhdunarodnogo prava v nacional'noe zakonodatel'stvo Respubliki Kazahstan. BULLETIN of L.N. Gumilyov Eurasian National University. LAW Series. No. 2 P. 113–123. DOI: 10.32523/2616-6844-2019-127-2-113-123 (In Russian)

9 V 2024-m zaregistrirovano bolee 17 tys. sluchaev internet-moshennichestva // Kazahstanskaja pravda. URL: https://kazpravda.kz/n/v-2024-m-zaregistrirovano-bolee-17-tys-sluchaev-internet-moshennichestva/ (data obrashhenija: 08.05.2026). (In Russian)

10 V Kazahstane raskryvaetsja lish' pjataja dolja internet-prestuplenij // PROFIT Online. URL: https://profit.kz/news/68399/V-Kazahstane-raskrivaetsya-lish-pyataya-dolya-internet-prestuplenij (data obrashhenija: 08.05.2026). (In Russian)

11 Chislo kiberprestuplenij v Kazahstane za 5 let vyroslo pochti v tri raza // Atameken Business. URL: https://www.inbusiness.kz/ru/last/chislo-kiberprestuplenij-v-kazahstane-za-5-let-vyroslo-pochti-v-tri-raza (data obrashhenija: 08.05.2026). (In Russian)

12 Keskin O. (2024) В Казахстане в 2023 году отразили 86,3 млн кибератак на ресурсы госорганов и важные объекты. URL: https://clck.su/obTbv (дата обращения: 08.05.2026). (In Russian)

13 General'naja prokuratura podvela itogi raboty za pervoe polugodie 2024 goda // Edinaja platforma internet-resursov gosudarstvennyh organov. URL: https://kazpravda.kz/n/generalnaya-prokuratura-podvela-itogi-raboty-za-pervoe-polugodie-2024-goda/ (data obrashhenija: 08.05.2026). (In Russian)

14 Brenner S.W. (2022) Cybercrime and the Law. Boston: Northeastern University Press. 412 p. (In English)

15 Clough J. (2021) Principles of Cybercrime. Cambridge: Cambridge University Press. 598 p. (In English)

16 Wall D. (2023) Cybercrime and Society. London: Sage Publications. 287 p. (In English)

17 Broadhurst R., Grabosky P. (2021) Cybercrime in Asia. Singapore: Springer. 355 p. (In English)

18 UNODC. Comprehensive Study on Cybercrime. Vienna: United Nations Office on Drugs and Crime, 2024. 320 p. (In English)

19 Europol. Internet Organised Crime Threat Assessment 2024. URL: https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024 (accessed: 08.05.2026). (In English)

20 Gordon S., Ford R. (2022) On the Definition and Classification of Cybercrime // Journal in Computer Virology. Vol. 18. No. 2. P. 145–159. (In English)

ЖАНДЫКЕЕВА Г.Е.,*[1]
PhD, аға оқытушы.
*e-mail: zhagulnar@gmail.com
ORCID ID: 0000-0003-3736-5292
ТОРГАУТОВА Б.А.,[2]
з.ғ.к., доцент.
e-mail: b.torgautova@etu.edu.kz
ORCID ID: 0000-0002-8793-3297
ЖАНДЫКЕЕВА А.К.,[3]
құқық магистрі.
e-mail: Azhandykeyeva@gmail.com
ORCID ID: 0009-0004-5497-1512
КУНДАКОВА М.Ж.,[4]
PhD, қауымдастырылған профессор.
e-mail: kundakovam@gmail.com
ORCID ID: 0009-0008-9846-4503
[1]Q University,
Алматы қ., Қазақстан
[2]META University,
Алматы қ., Қазақстан
[3]«Көпсалалы инновациялық колледж» ЖШС,
Алматы қ., Қазақстан
[4]ALT университеті,
Алматы қ., Қазақстан

ХАЛЫҚАРАЛЫҚ КИБЕРҚЫЛМЫСҚА ҚАРСЫ ІС-ҚИМЫЛ СТАНДАРТТАРЫН ҚАЗАҚСТАННЫҢ ҚЫЛМЫСТЫҚ ЗАҢНАМАСЫНА ИМПЛЕМЕНТАЦИЯЛАУ

Аңдатпа

Мақалада киберқылмысқа қарсы іс-қимылдың халықаралық стандарттарын Қазақстан Республикасының қылмыстық заңнамасына имплементациялау мәселелерінің теориялық және тәжірибелік қырлары қарастырылған. БҰҰ-ның Киберқылмысқа қарсы конвенциясының (2024 ж. редакциясы) ережелері мен Қазақстан Республикасының Қылмыстық және Қылмыстық-процестік кодекстерінің (2025 ж. редакциясы) нормаларына салыстырмалы-құқықтық талдау жүргізілді. Цифрландыру жағдайында қылмыстық-құ-

қықтық нормаларды тиімді қолдануға кедергі келтіретін олқылықтар мен сәйкессіздіктер анықталды. Қазақстан заңнамасы деректерді заңсыз ұстап алу, ақпараттық жүйелердің жұмысына араласу және өзге де цифрлық құқықбұзушылықтарға қатысты қылмыс құрамдарын тек ішінара қамтитыны белгілі болды. БҰҰ Конвенциясының 8–17 және 23–35-баптарына сәйкес келетін дербес қылмыс құрамдарын енгізу, сондай-ақ халықаралық ынтымақтастықтың процессуалдық тетіктерін және электрондық дәлелдемелермен жұмыс істеу тәртібін жетілдіру қажеттілігі негізделген. Ұлттық заңнаманы халықаралық нормалармен үйлестіру Қазақстан Республикасындағы цифрлық қауіпсіздікті нығайту мен қылмыстық сот төрелігінің тиімділігін арттырудың маңызды шарты болып табылатыны жөнінде қорытынды жасалған.

Тірек сөздер: киберқылмыс, заңнама, Конвенция, имплементация, қауіпсіздік, электрондық дәлелдемелер.

ZHANDYKEEVA G.E.,*[1]
PhD, senior lecturer.
*e-mail: zhagulnar@gmail.com
ORCID ID: 0000-0003-3736-5292
TORGAUTOVA B.A.,[2]
c.l.s., associate professor.
e-mail: b.torgautova@etu.edu.kz
ORCID ID: 0000-0002-8793-3297
ZHANDYKEEVA A.K.,[3]
master of law.
e-mail: Azhandykeyeva@gmail.com
ORCID ID: 0009-0004-5497-1512
KUNDAKOVA M.ZH.,[4]
PhD, associate professor.
e-mail: kundakovam@gmail.com
ORCID ID: 0009-0008-9846-4503
[1]Q University,
Almaty, Kazakhstan
[2]META University,
Almaty, Kazakhstan
[3]LLP Multidisciplinary
Innovation College,
Almaty, Kazakhstan
[4]ALT University,
Almaty, Kazakhstan

IMPLEMENTATION OF INTERNATIONAL STANDARDS FOR COUNTERING CYBERCRIME IN THE CRIMINAL LEGISLATION OF KAZAKHSTAN

Abstract

The article examines theoretical and practical issues of implementing international standards for combating cybercrime into the criminal legislation of the Republic of Kazakhstan. A comparative legal analysis of the provisions of the UN Convention against Cybercrime (2024 edition) and the norms of the Criminal and Criminal Procedure Codes of the Republic of Kazakhstan (2025 edition) is conducted. Gaps and inconsistencies that hinder the effective application of criminal law provisions in the context of digitalization are identified. It is revealed that Kazakhstani legislation only partially covers the elements of crimes related to illegal interception of data, interference with the functioning of information systems, and other forms of digital offenses. The need to introduce separate criminal offenses corresponding to Articles 8–17 and 23–35 of the UN Convention, as well as to improve procedural mechanisms for international cooperation and the handling of electronic evidence, has been substantiated. It concludes that harmonizing national legislation with international standards is an important condition for strengthening digital security and improving the effectiveness of criminal justice in the Republic of Kazakhstan.

Keywords: cybercrime, legislation, convention, implementation, security, electronic evidence.

Дата поступления статьи в редакцию: 14.04.2026