МРНТИ 10.81.00
УДК 343.791
JEL K49

https://doi.org/10.46914/2959-4197-2026-1-2-306-316

ТУЛЕУМУХАМБЕТОВ А.Б.,*[1]
докторант.
*e-mail: yntaka1988@gmail.com
ORCID ID: 0009-0000-9854-3246
ДИЛЬБАРХАНОВА Ж.Р.,[2]
д.ю.н., профессор.
e-mail: Dilbarkhanova@hotmail.com
ORCID ID: 0000-0003-3980-560X
[1]Алматинская академя МВД
Республики Казахстан
им. М. Есбулатова,
г. Алматы, Казахстан
[2]Академия управления МВД
Республики Казахстан,
г. Астана, Казахстан

ВОПРОСЫ ИНФОРМАЦИОННО-КОММУНИКАЦИОННОГО ОБЕСПЕЧЕНИЯ ПРОТИВОДЕЙСТВИЯ УГОЛОВНЫМ ПРАВОНАРУШЕНИЯМ В РЕСПУБЛИКЕ КАЗАХСТАН

Аннотация

В статье рассматривается эволюция и современное состояние механизма информационно-коммуникационного обеспечения противодействия уголовным правонарушениям в Республике Казахстан. Анализируются этапы становления и развития цифровых и информационно-аналитических систем органов внутренних дел, особенности внедрения центров оперативного управления. Особое внимание уделено нормативно-правовым основам защиты информации в условиях развития информационно-коммуникационных технологий, а также соотношению понятий «информационная безопасность», «киберпреступность» и «цифровая преступность», тем более что существуют по этому поводу различные взгляды ученых. Также необходимо учитывать современное состояние внедрения искусственного интеллекта и его применение в преступной среде. Это особенно важно при соотношении отличий данных понятий. Что сказывается и на расширении понятия информационной безопасности. На основе анализа национального законодательства и международных стандартов предлагаются уточненные авторские определения и направления совершенствования правового регулирования.

Ключевые слова: информационно-коммуникационные технологии, противодействие преступности, органы внутренних дел, информационная безопасность, киберпреступность, цифровая преступность.

Введение

Современное развитие информационно-коммуникационных технологий (далее – ИКТ) оказывает комплексное воздействие на все сферы общественной жизни, включая систему обеспечения правопорядка и безопасности. Цифровизация государственного управления, рост объемов электронных данных, распространение сетевых форм взаимодействия обусловили необходимость формирования эффективного механизма информационно-коммуникационного обеспечения противодействия уголовным правонарушениям. Для Республики Казахстан данная проблематика имеет особую актуальность в контексте реализации государственной политики цифровой трансформации и обеспечения информационной безопасности.

Целью настоящей статьи является комплексный анализ механизма информационно-коммуникационного обеспечения противодействия уголовным правонарушениям в Республике Казахстан. Данная цель ставит задачи по выявлению этапов его развития, а также обоснованию

направлений совершенствования нормативно-правового регулирования в условиях цифровизации.

Нормативноправовая база часто не успевает адаптироваться к быстро меняющимся технологическим реалиям. В некоторых случаях уголовное законодательство не в полном объеме регулирует вопросы противодействия преступлениям в сфере ИКТ. При этом ответственность за такие деяния разбросана по разным статьям, что осложняет квалификацию и расследование. Требуется унификация и систематизация подходов, а также разработка специализированных механизмов противодействия новым угрозам.

В науке также недостаточно проработаны теоретикоправовые аспекты использования ИКТ в преступной деятельности и как с ней бороться посредством ИКТ. Требуется развитие концепции киберкриминологии, уточнение понятийного аппарата ИКТ, изучение особенностей совершения таких преступлений и их уголовноправовой квалификации в рамках механизма противодействия, так как киберпреступления наносят значительный ущерб как отдельным гражданам, так и экономике государства в целом. Похищения средств, утечки данных, повреждения инфраструктуры приводят к финансовым потерям, снижению доверия к цифровым сервисам и замедлению цифровизации. Все это указывает на теоретическую и практическую значимость проводимого анализа.

Материалы и методы

Общенаучной методологической основой исследования являются положения общей закономерности и познания сущности существующего механизма информационно-коммуникационного обеспечения противодействия уголовным правонарушениям. В качестве частных научных методов познания использованы системно-структурный, логико-юридический, сравнительно-правовой, информационный, статистический, конкретно-социологический методы познания.

Материалами проводимого исследования выступает комплекс законодательных актов, государственных программ и стандартов, направленных на обеспечение информационной безопасности, защиту данных и регулирование цифровой сферы, которые составляют нормативно-правовую основу защиты в условиях развития информационно-коммуникационных технологий в Республике Казахстан. Исследование проводилось с помощью частнонаучных методов познания. Основной момент касается закона об информатизации и внесения некоторых поправок. Также исследование основывается на трудах зарубежных и отечественных авторов с помощью общенаучных методов познания.

Результаты и обсуждение

Информационно-коммуникационное обеспечение противодействия уголовным правонарушениям в Казахстане включает комплекс технологий, систем и образовательных программ, направленных на повышение эффективности работы правоохранительных органов. Ключевые элементы этого механизма включают Центры оперативного управления (ЦОУ); системы видеонаблюдения и видеоаналитики; электронный документооборот (СЭД); подготовку специалистов в области кибербезопасности и IT-криминалистики; сотрудничество правоохранительных органов с частными компаниями и международными организациями; законодательное регулирование.

Отметим, что данный механизм развивался в Республике Казахстан начиная с момента принятия независимости страны, который базировался на унаследованных от советского периода системах.

Начальный этап развития информационно-коммуникационного обеспечения органов внутренних дел МВД РК (1991–2000 гг.) характеризовался формированием базовых законодательных основ, началом внедрения компьютерных технологий и созданием первых инфраструктурных элементов для автоматизации процессов, а также формированием системы оперативно-разыскной деятельности. Этот период совпал с периодом становления независимого государства, что создавало как вызовы, так и возможности для модернизации правоохранительной системы.

Ключевым событием стало принятие Закона Республики Казахстан № 1405-XII «Об органах внутренних дел Республики Казахстан» 23 июня 1992 г. Этот акт определил задачи, функции, права и обязанности ОВД в новых условиях, заложив основу для дальнейшего развития правоохранительной системы. Однако он утратил силу в соответствии с Указом Президента Республики Казахстан от 21 декабря 1995 г. № 2707 о принятии Закона Республики Казахстан от 21 декабря 1995 г. № 2707 «Об органах внутренних дел Республики Казахстан» (с изменениями и дополнениями по состоянию на 7 марта 2014 г.). Он также в последующем утратил силу в соответствии с Законом РК от 23 апреля 2014 г. № 199-V [1]. В 1994 г. 15 сентября был принят Закон «Об оперативно-розыскной деятельности», который акцентировал внимание на развитии и улучшении оперативных служб [2]. Эти законодательные акты создали правовую базу для внедрения информационных технологий в деятельность МВД.

Отметим также, что именно в 1990-х годах в Казахстане началась последовательная работа по внедрению информационных технологий в систему государственного управления, включая правоохранительные органы, что заложило основы для дальнейшей цифровизации МВД РК. Так, были созданы первые центры оперативного управления (ЦОУ), компьютерные парки, началось формирование нормативно-правовой базы для использования информационных технологий в правоохранительной деятельности, появился опыт внедрения автоматизированных систем, который в последующие годы был масштабирован.

В последующие 10 лет (2000–2010 гг.) происходило активное развитие информационно-аналитических подразделений – были созданы специализированные информационные центры, внедрены первые электронные базы данных, формировалась система межведомственного взаимодействия.

Так, например, в 2003 г. был принят первый Закон РК «Об информатизации». Данный закон заложил основы государственного регулирования в сфере информатизации, включая принципы обеспечения информационной безопасности и требования к информационным системам, также способствовал стандартизации и централизации процессов в правоохранительных органах. Однако в последующем он утратил силу в соответствии с принятием Закона РК от 11 января 2007 г. № 217-III [3], который также утратил силу в 2015 г. в связи с принятием нового закона об информатизации РК [4].

Современный этап развития информационно-коммуникационного обеспечения МВД РК с 2011 г. по настоящее время характеризуется масштабной цифровизацией, дальнейшим внедрением передовых технологий и переходом к сервисной модели полиции. Ключевые направления включают совершенствование ЦОУ, автоматизацию документооборота, развитие систем видеонаблюдения и аналитики, а также подготовку кадров в сфере IT. Учебные заведения МВД РК активно внедряют программы подготовки специалистов в сфере IT, киберпреступности, экстремизма и финансовых преступлений. Так, например, в Алматинской академии МВД РК имени М. Есболатова создан Центр по подготовке специалистов по противодействию киберпреступности, в Карагандинской академии МВД РК имени Б. Бейсенова образована кафедра кибербезопасности.

В целях противодействия транснациональной преступности Казахстан активно сотрудничает с Интерполом, Европолом и другими международными организациями. Внедряются международные стандарты в управлении полицейскими данными, системы автоматизированного учета и анализа преступлений.

Таким образом, на сегодняшний день информационно-коммуникационное обеспечение МВД РК представляет собой комплексную систему, включающую современные технологии и методы работы. Продолжается процесс модернизации и совершенствования не только информационных систем с учетом новых вызовов и угроз, но и нормативно-правового обеспечения в этой области.

Нормативно-правовые основы защиты в условиях развития информационно-коммуникационных технологий в Республике Казахстан включают комплекс законодательных актов, государственных программ и стандартов, направленных на обеспечение информационной безопасности, защиту данных и регулирование цифровой сферы.

Ключевыми документами в этой области выступают:

1. Закон Республики Казахстан «Об информатизации» от 24 ноября 2015 г. № 418-V ЗРК.

2. Концепция цифровой трансформации, развития отрасли ИКТ и кибербезопасности на 2023–2029 гг. утверждена Постановлением Правительства РК от 28 марта 2023 г. № 269.

3. Концепция кибербезопасности («Киберщит Казахстана») [5].

4. Постановление Правительства РК от 20 декабря 2016 г. № 832 «Об утверждении единых требований в области ИКТ и обеспечения информационной безопасности». Так же как и Постановление Правительства РК от 13 мая 2024 г. №372 «О внесении изменений и дополнений в постановление Правительства Республики Казахстан от 20 декабря 2016 года № 832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности»» устанавливает правила организации информационной безопасности, включая требования к защите активов, управлению доступом, регистрации инцидентов и другие аспекты [6].

5. Закон «О персональных данных и их защите» от 21 мая 2013 г. № 94-V [7].

6. Закон Республики Казахстан «О доступе к информации» от 16 ноября 2015 г. № 401-V ЗРК [8].

7. Уголовный кодекс Республики Казахстан (далее – УК РК) от 3 июля 2014 г. № 226-V (с изменениями и дополнениями по состоянию на 16.09.2025). Содержит отдельную главу 7, посвященную преступлениям в сфере информатизации и связи. По состоянию на 16 сентября 2025 г. эта глава включает статьи, регулирующие ответственность за различные составы преступлений против электронных информационных ресурсов и систем [9]. Сюда также можно отнести и ряд других составов уголовных правонарушений, связанных с информационно-коммуникационным обеспечением (29).

8. Кодекс Республики Казахстан об административных правонарушениях (далее – КобАП РК) от 5 июля 2014 г. № 235-V (с изменениями и дополнениями по состоянию на 15.09.2025 г.) [10].

9. Государственные стандарты Республики Казахстан (например, СТ РК ISO/IEC 27002-2023, СТ РК ИСО/МЭК 17799-2006, СТ РК ИСО/МЭК 27001-2008).

10. Национальный антикризисный план реагирования на инциденты информационной безопасности. Утверждается Правительством РК и включает меры по оперативному реагированию на кибератаки и другие угрозы [11].

11. Деятельность специализированных организаций. Например, Национальная служба реагирования на компьютерные инциденты (KZ-CERT) занимается мониторингом и реагированием на инциденты, а Национальный координационный центр информационной безопасности защищает критически важные объекты.

Особенно хотелось бы отметить принятые в последнее время новые законы – Закон Республики Казахстан «Об искусственном интеллекте» 2025 г. [12], Закон Республики Казахстан «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам искусственного интеллекта и цифровизации» от 17 ноября 2025 г. [13], Цифровой кодекс РК (вступит в силу по истечении 6 месяцев) [14] и ряд других мер (например, Концепция развития искусственного интеллекта до 2029 г. [15], а также объявление 2026 года Годом цифровизации и искусственного интеллекта).

Кроме того, нормативно-правовые акты различных ведомств, чья деятельность непосредственно связана с информационно-коммуникационным обеспечением, например приказ министра цифрового развития, оборонной и аэрокосмической промышленности Республики Казахстан от 3 июня 2019 г. № 111/НҚ «Об утверждении методики и правил проведения испытаний объектов информатизации «электронного правительства» и информационных систем, отнесенных к критически важным объектам информационно-коммуникационной инфраструктуры, на соответствие требованиям информационной безопасности», приказ и.о. министра по инвестициям и развитию Республики Казахстан от 28 января 2016 г. № 135 «Об утверждении Правил классификации объектов информатизации и классификатор объектов информатизации», приказ и.о. министра информации и коммуникаций Республики Казахстан от 29 марта 2018 г. № 123 «Об утверждении Правил интеграции объектов информатизации «электронного правительства».

Эти нормативные акты составляют единую систему защиты в цифровой среде, охватывающую как государственные, так и частные информационные ресурсы. Они направлены на обеспечение стабильности, безопасности и развития ИКТ-сферы в Казахстане.

Однако проведенный анализ вышеприведенных нормативно-правовых актов показал, что в них нет объединяющего определения понятий «информационная безопасность», «киберпреступность» и «цифровая преступность», которые по своей сути существенно различаются. Вместе с тем, их объединяет непосредственная связь с понятием «информационно-коммуникационные технологии».

Начнем с того, что цифровая преступность связана с цифровыми технологиями, под которыми понимается комплекс инновационных средств, основанных на представлении информации в цифровой форме (биты, байты, двоичный код), использовании компьютеров и электронных устройств для обработки, хранения, передачи и анализа данных, применении сетевых инфраструктур для связи и обмена информацией между системами и пользователями. То есть это гаджеты, электронные устройства, технологии, программы [16]. Но их часто путают с информационными, но на самом деле одно является частью другого. Информационные технологии (ИТ) – более широкое понятие, включающее цифровые технологии как ключевой элемент.

К информационным относят все технологии, связанные с обменом информацией, даже с помощью аналоговых устройств. Например, светофор, сообщающий нам, когда можно идти, – это информационное аналоговое устройство, а сервис, где мы отслеживаем пробки, тоже информационное, но уже цифровое. То есть это процесс, использующий совокупность средств и методов сбора, обработки и передачи данных (первичной информации) для получения информации нового качества о состоянии объекта, процесса или явления (информационного продукта) [17].

При этом отметим, что цифровая преступность более широкое понятие, чем киберпреступность. Так как она включает не только преступления, совершаемые с помощью цифровых технологий, но и те, где цифровые данные или инфраструктура являются объектом посягательства. Например, незаконное распространение информации в Интернете, кибersталкинг, торговля цифровыми активами (криптовалютой).

В свою очередь, киберпреступность – совокупность преступлений, совершаемых с использованием компьютерных систем, сетей или цифровых технологий. К ним относятся, например, фишинг, хакерские атаки, распространение вредоносного ПО, кибершпионаж, мошенничество с электронными платежами. Киберпреступность часто связана с нарушением работы информационных систем и хищением данных.

Это подкрепляется рядом международных документов, где напрямую дается анализ киберпреступности. Однако законодательного определения нет. Так, например, в Конвенции Совета Европы «О киберпреступности» 2001 г. термин «cybercrime» подразумевает действия, направленные против конфиденциальности, целостности и доступности компьютерных систем и сетей и компьютерных данных, а также против злоупотребления такими системами, сетями и данными путем обеспечения уголовной наказуемости таких деяний [18].

При этом, как отмечают зарубежные ученые, современную киберпреступность стоит называть уже «преступность в сфере искусственного интеллекта, или ИИ-преступность» [19]. И делят ее на три вида – преступления, совершаемые при помощи ИИ, где ИИ является объектом и где ИИ является субъектом [20]. Однако данный вопрос необходимо рассматривать глубже. Поэтому углубляться в рамках статьи не будем.

Связью между этим понятиями выступает информационная безопасность. Она является средством противодействия кибер- и цифровой преступности. Киберпреступность и цифровая преступность представляют собой угрозы, на которые направлена система информационной безопасности. Эффективная информационная безопасность требует учета специфики цифровых преступлений, включая их транснациональный характер, использование сложных технологий и постоянное развитие новых методов атак.

То есть информационная безопасность (ИБ) – основа, которая охватывает защиту информации от несанкционированного доступа, изменения, уничтожения или нарушения доступности. Включает технические, организационные и правовые меры, направленные на обеспечение конфиденциальности, целостности и доступности данных.

Согласно п. 7 ст. 1 закона об информатизации, информационная безопасность в сфере информатизации – состояние защищенности электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры от внешних и внутренних угроз [4].

В современных условиях информационная безопасность охватывает не только цифровые данные, но и физические носители, а также процессы обработки информации. Она включает защиту от кибератак, вредоносного ПО, фишинга, DDoS-атак и других угроз, а также соблюдение законодательства в сфере защиты данных (например, требований к шифрованию, уведомлению об утечках).

Таким образом, информационная безопасность – это комплекс мер, методов, процедур и технологий для защиты информации от несанкционированного доступа, искажения, уничтожения или разглашения, обеспечивающий ее конфиденциальность, целостность и доступность (принцип КЦД) как в цифровом, так и в физическом виде. Это широкое понятие, включающее кибербезопасность, защиту данных на любых носителях (от бумаг до серверов) и защиту интересов личности, общества и государства.

Поэтому, на наш взгляд, законодательное определение должно быть немного шире. Оно должно включать состояние защищенности информационных систем, данных и инфраструктуры как в цифровом, так и в физическом виде от несанкционированного доступа, изменения, уничтожения или утечки, обеспечиваемое комплексом технических, организационных и правовых мер.

Тем более что законодательное понятие намного ближе к понятию кибербезопасности, которое, в свою очередь, фокусируется на цифровых угрозах (вирусы, хакеры, фишинг), тогда как информационная безопасность шире – она охватывает и защиту физических носителей (например, кража бумажных документов), а также общие процессы работы с информацией.

Предлагаем п. 7 ст. 1 закона об информатизации дать в следующей редакции: «информационная безопасность – это состояние защищенности информационных систем, данных и инфраструктуры как в цифровом, так и в физическом виде от несанкционированного доступа, изменения, уничтожения или утечки, обеспечиваемое комплексом технических, организационных и правовых мер», что будет намного шире, чем указано в законе.

При этом информационная безопасность в контексте противодействия кибер- и цифровой преступности – это система мер, технологий и процедур, направленных на защиту информации, информационных систем и инфраструктуры от угроз, связанных с противоправными действиями в цифровом пространстве, включая кибератаки, мошенничество, распространение вредоносного ПО и другие формы цифровых преступлений. Она включает обеспечение конфиденциальности, целостности и доступности данных, а также предотвращение, обнаружение и нейтрализацию угроз, возникающих в результате использования современных технологий для преступных целей.

Основным средством информационной безопасности, так же как компонентом кибер- и цифровой преступности, выступают информационнокоммуникационные технологии (ИКТ). То есть это интегрированная область цифровых технологий, обеспечивающая:

- производство, хранение и обработку информации;
- ее электронное распространение и обмен;
- коммуникацию между пользователями и системами в реальном времени.

Ключевой признак ИКТ – сочетание информационных (работа с данными) и коммуникационных (связь и передача) функций в единой технологической среде.

Согласно п. 28 ст. 1 Закона РК «Об информатизации» от 24 ноября 2015 г. № 418-V, информационно-коммуникационные технологии – совокупность методов работы с электронными информационными ресурсами и методов информационного взаимодействия, осуществляемых с применением аппаратно-программного комплекса и сети телекоммуникаций.

Однако, на наш взгляд, данное определение является не совсем точным. Так как методы работы с электронными информационными ресурсами (ЭИР) – это навыки поиска, отбора, анализа и использования данных в цифровом виде (тексты, базы данных, медиа) с помощью ИКТ. Методы информационного взаимодействия – это способы обмена данными между пользователем и системой, а также между системами через телекоммуникации (Интернет, сети),

реализующие сбор, обработку и передачу информации для коммуникации. То есть в общем смысле методы и в том, и в ином случае – это работа или род деятельности с информационными данными.

В ходе проведенного анализа нормативно-правовых актов, определений и мнений ученых-юристов, сформулировано определение: информационно-коммуникационные технологии – это основные компоненты технологической среды, используемые для информационного взаимодействия на основе методов работы с электронно-информационными ресурсами посредством коммуникации между пользователями и системами в реальном времени. Это определение предлагается изложить в п. 28 ст. 1 Закона РК об информатизации в представленной редакции.

Заключение

Таким образом, проведенное исследование позволило установить, что механизм информационно-коммуникационного обеспечения противодействия уголовным правонарушениям в Республике Казахстан представляет собой сложную, многоуровневую систему, включающую нормативно-правовые, организационные и технологические компоненты, функционирующие в условиях цифровой трансформации общества.

Анализ этапов развития данного механизма показал его эволюцию от фрагментарного внедрения информационных технологий в деятельность органов внутренних дел к формированию интегрированной цифровой инфраструктуры, обеспечивающей обработку и использование значительных массивов данных, межведомственное взаимодействие и повышение эффективности правоохранительной деятельности.

Также установлено, что современное состояние правового регулирования в сфере информационно-коммуникационных технологий характеризуется значительным расширением нормативной базы, включая принятие новых законодательных актов, регулирующих вопросы цифровизации, кибербезопасности и использования искусственного интеллекта. Вместе с тем выявлены отдельные проблемы, связанные с фрагментарностью правового регулирования и отсутствием единообразного понятийного аппарата, что затрудняет правоприменительную практику и требует дальнейшего научного осмысления.

Особое значение имеет разграничение понятий «информационная безопасность», «киберпреступность» и «цифровая преступность», поскольку их смешение в законодательстве и научной доктрине снижает эффективность противодействия соответствующим видам правонарушений.

В рамках исследования нами предложено авторское определение информационно-коммуникационных технологий, направленное на уточнение понятийного аппарата и совершенствование законодательства Республики Казахстан в данной сфере.

ЛИТЕРАТУРА

1 Закон Республики Казахстан от 23 апреля 2014 года № 199-V «Об органах внутренних дел Республики Казахстан» (с изменениями и дополнениями по состоянию на 20.11.2025 г.). URL: https://online.zakon.kz/Document/?doc_id=1004063&doc_id2=31538985#pos=3;-98&pos2=489;-62 (дата обращения: 24.01.2026)

2 Закон Республики Казахстан от 15 сентября 1994 года № 154-XIII «Об оперативно-розыскной деятельности» (с изменениями и дополнениями по состоянию на 16.09.2025 г.). URL: https://online.zakon.kz/Document/?doc_id=1003158 (дата обращения: 24.01.2026)

3 Закон Республики Казахстан от 11 января 2007 года № 217-III «Об информатизации» (с изменениями и дополнениями по состоянию на 31.10.2015 г.) (утратил силу). URL: https://online.zakon.kz/Document/?doc_id=1039543&doc_id2=30085759#pos=5;-98&pos2=650;-44 (дата обращения: 24.01.2026)

4 Закон Республики Казахстан от 24 ноября 2015 года № 418-V ЗРК «Об информатизации». URL: https://adilet.zan.kz/rus/docs/Z1500000418 (дата обращения: 24.01.2026)

5 Об утверждении Концепции кибербезопасности («Киберщит Казахстана»). Постановление Правительства Республики Казахстан от 30 июня 2017 года № 407. URL: https://adilet.zan.kz/rus/docs/P1700000407 (дата обращения: 24.01.2026)

6 О внесении изменений и дополнений в постановление Правительства Республики Казахстан от 20 декабря 2016 года № 832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности». Постановление Правительства Республики Казахстан от 13 мая 2024 года № 372. URL: https://adilet.zan.kz/rus/docs/P2400000372/links (дата обращения: 24.01.2026)

7 Закон Республики Казахстан от 21 мая 2013 года № 94-V «О персональных данных и их защите». URL: https://adilet.zan.kz/rus/docs/Z1300000094 (дата обращения: 24.01.2026)

8 Закон Республики Казахстан от 16 ноября 2015 года № 401-V «О доступе к информации» (с изменениями и дополнениями по состоянию на 16.03.2025 г.). URL: https://online.zakon.kz/Document/?doc_id=39415981 (дата обращения: 24.01.2026)

9 Уголовный кодекс Республики Казахстан от 3 июля 2014 года № 226-V (с изменениями и дополнениями по состоянию на 16.09.2025 г.). URL: https://online.zakon.kz/Document/?doc_id=31575252&pos=5;-106#pos=5;-106 (дата обращения: 24.01.2026)

10 Кодекс Республики Казахстан об административных правонарушениях от 5 июля 2014 года № 235-V (с изменениями и дополнениями по состоянию на 15.09.2025 г.). URL: https://online.zakon.kz/Document/?doc_id=31577399&doc_id2=31575252#pos=1942;-80&pos2=2668;-80 (дата обращения: 24.01.2026)

11 Об утверждении Национального антикризисного плана реагирования на инциденты информационной безопасности: Постановление Правительства Республики Казахстан от 9 августа 2018 года № 488. URL: https://adilet.zan.kz/rus/docs/P1800000488 (дата обращения: 24.01.2026)

12 Закон Республики Казахстан от 17 ноября 2025 года № 230-VIII ЗРК «Об искусственном интеллекте». URL: https://adilet.zan.kz/rus/docs/Z2500000230 (дата обращения: 24.01.2026)

13 Закон Республики Казахстан «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам искусственного интеллекта и цифровизации» от 17 ноября 2025 года № 231-VIII ЗРК // Казахстанская правда. – 2025. – 18 ноября. – № 222 (30600)

14 Кодекс Республики Казахстан от 9 января 2026 года № 255-VIII «Цифровой кодекс Республики Казахстан» (не введен в действие) // ИПС «Параграф». URL: https://prg.kz/document/?doc_id=38546537 (дата обращения: 24.01.2026)

15 Об утверждении Концепции развития искусственного интеллекта на 2024–2029 годы: Постановление Правительства Республики Казахстан от 24 июля 2024 года № 592. URL: https://adilet.zan.kz/rus/docs/P2400000592 (дата обращения 24.01.2026)

16 Почему цифровые технологии вытесняют аналоговые. URL: https://trends.rbc.ru/trends/industry/60e427ea9a79471089a0ec1d (дата обращения: 24.01.2026)

17 Суперкомпьютерные технологии: СКТ-2014 материалы 3-й Всероссийской научно-технической конференции (29 сентября – 4 октября 2014, Дивноморское, Геленджик). – Ростов-на-Дону: Изд-во Южного федерального университета, 2014. – 274 с.

18 Convention on Cybercrime Council of Europe. 2001. URL: https://www.coe.int/en/web/conventions/full-list/-/conventions/ treaty/185?module=treaty-detail&treatynum=185 (accessed: 25.03.2026)

19 Spyropoulos F. New Approaches to Researching AI Crime: Institutionalization of Digital Criminology // Journal of Digital Technologies and Law. 2024. V. 2. No. 3. P. 636–656. DOI: 0.21202/jdtl.2024.32.

20 Brundage M., Avin S., Clark J. et al. The malicious use of artificial intelligence. 2018. URL: https://clck.ru/3CzSuH // https://arxiv.org/ftp/arxiv/papers/1802/1802.07228.pdf (accessed: 13.04.2026)

REFERENCES

1 Zakon Respubliki Kazahstan ot 23 aprelja 2014 goda No. 199-V «Ob organah vnutrennih del Respubliki Kazahstan» (s izmenenijami i dopolnenijami po sostojaniju na 20.11.2025 g.). URL: https://online.zakon.kz/Document/?doc_id=1004063&doc_id2=31538985#pos=3;-98&pos2=489;-62 (data obrashhenija: 24.01.2026). (In Russian)

2 Zakon Respubliki Kazahstan ot 15 sentjabrja 1994 goda No. 154-XIII «Ob operativno-rozysknoj dejatel'nosti» (s izmenenijami i dopolnenijami po sostojaniju na 16.09.2025 g.). URL: https://online.zakon.kz/Document/?doc_id=1003158 (data obrashhenija: 24.01.2026). (In Russian)

3 Zakon Respubliki Kazahstan ot 11 janvarja 2007 goda No. 217-III «Ob informatizacii» (s izmenenijami i dopolnenijami po sostojaniju na 31.10.2015 g.) (utratil silu). URL: https://online.zakon.kz/Document/?doc_id=1039543&doc_id2=30085759#pos=5;-98&pos2=650;-44 (data obrashhenija: 24.01.2026). (In Russian)

4 Zakon Respubliki Kazahstan ot 24 nojabrja 2015 goda No. 418-V ZRK «Ob informatizacii». URL: https://adilet.zan.kz/rus/docs/Z1500000418 (data obrashhenija: 24.01.2026). (In Russian)

5 Ob utverzhdenii Koncepcii kiberbezopasnosti («Kibershhit Kazahstana»). Postanovlenie Pravitel'stva Respubliki Kazahstan ot 30 ijunja 2017 goda No. 407. URL: https://adilet.zan.kz/rus/docs/P1700000407 (data obrashhenija: 24.01.2026). (In Russian)

6 O vnesenii izmenenij i dopolnenij v postanovlenie Pravitel'stva Respubliki Kazahstan ot 20 dekabrja 2016 goda No. 832 «Ob utverzhdenii edinyh trebovanij v oblasti informacionno-kommunikacionnyh tehnologij i obespechenija informacionnoj bezopasnosti». Postanovlenie Pravitel'stva Respubliki Kazahstan ot 13 maja 2024 goda № 372. URL: https://adilet.zan.kz/rus/docs/P2400000372/links (data obrashhenija: 24.01.2026). (In Russian)

7 Zakon Respubliki Kazahstan ot 21 maja 2013 goda No. 94-V «O personal'nyh dannyh i ih zashhite». URL: https://adilet.zan.kz/rus/docs/Z1300000094 (data obrashhenija: 24.01.2026). (In Russian)

8 Zakon Respubliki Kazahstan ot 16 nojabrja 2015 goda No. 401-V «O dostupe k informacii» (s izmenenijami i dopolnenijami po sostojaniju na 16.03.2025 g.). URL: https://online.zakon.kz/Document/?doc_id=39415981 (data obrashhenija: 24.01.2026). (In Russian)

9 Ugolovnyj kodeks Respubliki Kazahstan ot 3 ijulja 2014 goda No. 226-V (s izmenenijami i dopolnenijami po sostojaniju na 16.09.2025 g.). URL: https://online.zakon.kz/Document/?doc_id=31575252&pos=5;-106#pos=5;-106 (data obrashhenija: 24.01.2026). (In Russian)

10 Kodeks Respubliki Kazahstan ob administrativnyh pravonarushenijah ot 5 ijulja 2014 goda No. 235-V (s izmenenijami i dopolnenijami po sostojaniju na 15.09.2025 g.). URL: https://online.zakon.kz/Document/?doc_id=31577399&doc_id2=31575252#pos=1942;-80&pos2=2668;-80 (data obrashhenija: 24.01.2026). (In Russian)

11 Ob utverzhdenii Nacional'nogo antikrizisnogo plana reagirovanija na incidenty informacionnoj bezopasnosti: Postanovlenie Pravitel'stva Respubliki Kazahstan ot 9 avgusta 2018 goda No. 488. URL: https://adilet.zan.kz/rus/docs/P1800000488 (data obrashhenija: 24.01.2026). (In Russian)

12 Zakon Respubliki Kazahstan ot 17 nojabrja 2025 goda No. 230-VIII ZRK «Ob iskusstvennom intellekte». URL: https://adilet.zan.kz/rus/docs/Z2500000230 (data obrashhenija: 24.01.2026). (In Russian)

13 Zakon Respubliki Kazahstan «O vnesenii izmenenij i dopolnenij v nekotorye zakonodatel'nye akty Respubliki Kazahstan po voprosam iskusstvennogo intellekta i cifrovizacii» ot 17 nojabrja 2025 goda № 231-VIII ZRK // Kazahstanskaja pravda. 2025. 18 nojabrja. No. 222 (30600). (In Russian)

14 Kodeks Respubliki Kazahstan ot 9 janvarja 2026 goda № 255-VIII «Cifrovoj kodeks Respubliki Kazahstan» (ne vveden v dejstvie) // IPS «Paragraf». URL: https://prg.kz/document/?doc_id=38546537 (data obrashhenija: 24.01.2026). (In Russian)

15 Ob utverzhdenii Koncepcii razvitija iskusstvennogo intellekta na 2024–2029 gody: Postanovlenie Pravitel'stva Respubliki Kazahstan ot 24 ijulja 2024 goda No. 592. URL: https://adilet.zan.kz/rus/docs/P2400000592 (data obrashhenija 24.01.2026). (In Russian)

16 Pochemu cifrovye tehnologii vytesnjajut analogovye. URL: https://trends.rbc.ru/trends/industry/60e427ea9a79471089a0ec1d (data obrashhenija: 24.01.2026). (In Russian)

17 Superkomp'juternye tehnologii: SKT-2014 materialy 3-j Vserossijskoj nauchno-tehnicheskoj konferencii (29 sentjabrja – 4 oktjabrja 2014, Divnomorskoe, Gelendzhik). Rostov-na-Donu: Izd-vo Juzhnogo federal'nogo universiteta, 2014. 274 p. (In Russian)

18 Convention on Cybercrime Council of Europe. 2001. URL: https://www.coe.int/en/web/conventions/full-list/-/conventions/ treaty/185?module=treaty-detail&treatynum=185 (accessed: 25.03.2026). (In English)

19 Spyropoulos F. (2024) New Approaches to Researching AI Crime: Institutionalization of Digital Criminology // Journal of Digital Technologies and Law. V. 2. No. 3. P. 636–656. URL: DOI: 0.21202/jdtl.2024.32 In English)

20 Brundage M., Avin S., Clark J. et al. (2018) The malicious use of artificial intelligence. URL: https://clck.ru/3CzSuH // https://arxiv.org/ftp/arxiv/papers/1802/1802.07228.pdf (accessed: 13.04.2026). (In English)

ТУЛЕУМУХАМБЕТОВ А.Б.,*[1]
докторант.
*e-mail: yntaka1988@gmail.com
ORCID ID: 0009-0000-9854-3246
ДИЛЬБАРХАНОВА Ж.Р.,[2]
з.ғ.д., профессор.
e-mail:Dilbarkhanova@hotmail.com
ORCID ID: 0000-0003-3980-560X
[1]Қазақстан Республикасы Ішкі істер
министрлігінің М. Есболатов
атындағы Алматы академиясы,
Алматы қ., Қазақстан
[2]Қазақстан Республикасы
Ішкі істер министрлігінің
Басқару академиясы,
Астана қ., Қазақстан

ҚАЗАҚСТАН НЕСПУБЛИКАСЫНДА ҚЫЛМЫСТЫҚ ҚҰҚЫҚ БҰЗУШЫЛЫҚТАРҒА ҚАРСЫ ІС-ҚИМЫЛДЫ АҚПАРАТТЫҚ-КОММУНИКАЦИЯЛЫҚ ҚАМТАМАСЫЗ ЕТУ МӘСЕЛЕЛЕРІ

Аңдатпа

Мақалада Қазақстан Республикасындағы қылмыстық құқық бұзушылықтарға қарсы іс-қимылды ақпараттық-коммуникациялық қамтамасыз ету тетігінің эволюциясы мен қазіргі жағдайы қарастырылады. Ішкі істер органдарының цифрлық және ақпараттық-талдамалық жүйелерінің қалыптасу және даму кезеңдері, жедел басқару орталықтарын енгізу ерекшеліктері талданады. Ақпараттық-коммуникациялық технологиялардың дамуы жағдайында ақпаратты қорғаудың нормативтік-құқықтық негіздеріне, сондай-ақ «ақпараттық қауіпсіздік», «киберқылмыс» және «цифрлық қылмыс» ұғымдарының арақатынасына ерекше назар аударылады. Халықаралық құжаттарда киберқылмыстың немесе цифрлық қылмыстың заңмен бекітілген анықтамасы жоқ екені анықталды. Сонымен қатар, бұл туралы ғалымдардың әртүрлі көзқарастары бар. Сондай-ақ, жасанды интеллектті енгізудің және оны қылмыстық ортада қолданудың қазіргі жағдайын ескеру қажет. Бұл әсіресе осы ұғымдардың айырмашылықтарының арақатынасында өте маңызды. Ақпараттық қауіпсіздік ұғымын кеңейтуге не әсер етеді. Ұлттық заңнама мен халықаралық стандарттарды талдау негізінде авторлық анықтамалар нақтыланып, құқықтық реттеуді жетілдіру бағыттары ұсынылады.

Тірек сөздер: ақпараттық-коммуникациялық технологиялар, қылмысқа қарсы іс-қимыл, ішкі істер органдары, ақпараттық қауіпсіздік, киберқылмыс, цифрлық қылмыс.

TULEUMUKHAMBETOV A.B.,*[1]
PhD student.
*e-mail: yntaka1988@gmail.com
ORCID ID: 0009-0000-9854-3246
DILBARKHANOVA Z.R.,[2]
d.l.s., professor.
e-mail: Dilbarkhanova@hotmail.com
ORCID ID: 0000-0003-3980-560X
[1]Almaty Academy of the Ministry
of Internal Affairs named after M. Esbulatov,
Almaty, Kazakhstan
[2]Management Academy
of the Ministry of Internal Affairs
of the Republic of Kazakhstan,
Astana, Kazakhstan

ISSUES OF INFORMATION AND COMMUNICATION SUPPORT FOR COUNTERING CRIMINAL OFFENSES IN THE REPUBLIC OF KAZAKHSTAN

Abstract

The article examines the evolution and current state of the mechanism of information and communication support for countering criminal offences in the Republic of Kazakhstan. The stages of formation and development of digital and

information-analytical systems of internal affairs bodies, as well as the features of implementing operational control centers, are analyzed. Particular attention is paid to the regulatory and legal framework for information protection in the context of the development of information and communication technologies, as well as to the correlation between the concepts of “information security,” “cybercrime,” and “digital crime.” It has been revealed that international documents lack a statutory definition of cybercrime or digital crime. Moreover, scholars hold differing views on this matter. It is also necessary to consider the current state of artificial intelligence implementation and its application in the criminal environment. This is particularly important when balancing the differences between these concepts. This also impacts the expansion of the concept of information security. Based on the analysis of national legislation and international standards, refined author’s definitions and directions for improving legal regulation are proposed.

Keywords: information and communication technologies, crime prevention, internal affairs bodies, information security, cybercrime, digital crime.

Дата поступления статьи в редакцию: 07.04.2026