МРНТИ 10.79.35 DOI: https://doi.org/10.62687/VLJ.1.2.2026.27

ОБ ЭФФЕКТИВНЫХ СПОСОБАХ ЗАЩИТЫ ИНТЕРЕСОВ ГРАЖДАН, СТАВШИХ ЖЕРТВАМИ ИНТЕРНЕТ – МОШЕННИЧЕСТВА

М.Ж. Омарбекова*
Верховный Суд РК, г. Астана, Казахстан
*e-mail: madeniyeto@mail.ru

М.Ж. Омарбекова – судья Верховного Суда Республики Казахстан, кандидат юридических наук, профессор Академии правосудия при Высшем Судебном Совете Республики Казахстан; г. Астана, Республика Казахстан; ORCID ID: https://orcid.org/0009-0007-1323-9597; e-mail: madeniyeto@mail.ru

Аннотация. В статье рассматриваются вопросы совершенствования уголовно-процессуального регулирования в Республике Казахстан в связи с ростом киберпреступности и развитием международного сотрудничества в данной сфере. Анализируются стратегические документы в области кибербезопасности (Концепция кибербезопасности «Киберщит Казахстана», Концепция цифровой трансформации, развития ИКТ и кибербезопасности на 2023–2029 годы), показано значение присоединения Республики Казахстан к Будапештской конвенции о компьютерных преступлениях и Конвенции ООН против киберпреступности для упрощения трансграничного доступа к электронным доказательствам и проведения оперативного международного взаимодействия. Отмечено, что действующее уголовно-процессуальное законодательство содержит лишь фрагментарное регулирование электронных документов и компьютерной информации, что не соответствует практическим потребностям раскрытия и расследования киберпреступлений. Обосновывается необходимость нормативного закрепления понятия электронных доказательств, их классификации в зависимости от места хранения, а также специальных процессуальных механизмов их получения, обеспечения сохранности, изъятия и использования в уголовном судопроизводстве с учётом международных стандартов.

Ключевые слова: киберпреступность, преступления в сфере информационной безопасности, электронное доказательство, уголовные правонарушения, сфера информатизации и связи, интернет-мошенничество, уголовная ответственность.

ИНТЕРНЕТ АЛАЯҚТЫҚТАН ЗАРДАП ШЕККЕН АЗАМАТТАРДЫҢ МҮДДЕЛЕРІН ҚОРҒАУДЫҢ ТИІМДІ ТӘСІЛДЕРІ

М.Ж. Омарбекова*
ҚР Жоғарғы Соты, Астана, Қазақстан
*e-mail: madeniyeto@mail.ru

М.Ж. Омарбекова – Қазақстан Республикасы Жоғарғы Сотының судьясы, заң ғылымдарының кандидаты, Қазақстан Республикасы Жоғарғы Сот Кеңесі жанындағы Сот төрелігі академиясының профессоры; Астана, Қазақстан Республикасы; ORCID ID: https://orcid.org/0009-0007-1323-9597; e-mail: madeniyeto@mail.ru

Андатпа. Мақалада Қазақстан Республикасында киберқылмыстылықтың өсуі және осы саладағы халықаралық ынтымақтастықтың дамуына байланысты қылмыстық іс жүргізу саласындағы құқықтық реттеуді жетілдіру мәселелері қарастырылады. Киберқауіпсіздік саласындағы стратегиялық құжаттарға (киберқауіпсіздік жөніндегі «Қазақстанның киберқалқаны» тұжырымдамасы, 2023–2029 жылдарға арналған цифрлық трансформация, АКТ-ны және киберқауіпсіздікті дамыту тұжырымдамасы) талдау жүргізіледі, сондай-ақ электрондық дәлелдемелерге трансшекаралық қолжетімділікті жеңілдету және

жедел халықаралық өзара іс-қимылды қамтамасыз ету үшін Қазақстан Республикасының компьютерлік қылмыстар туралы Будапешт конвенциясына және БҰҰ-ның киберқылмысқа қарсы конвенциясына қосылуының маңызы айқындалады. Қолданыстағы қылмыстық іс жүргізу заңнамасы электрондық құжаттар мен компьютерлік ақпаратты реттеуді тек фрагменттік түрде көздейтіні, бұл киберқылмыстарды ашу және тергеудің практикалық қажеттіліктеріне толық көлемде сәйкес келмейтіні атап өтіледі. Халықаралық стандарттарды ескере отырып, электрондық дәлелдеме ұғымын нормативтік тұрғыдан бекіту, оларды сақталу орнына қарай жіктеу, сондай-ақ оларды алу, сақталуын қамтамасыз ету, тәркілеу және қылмыстық сот ісін жүргізуде пайдалану бойынша арнайы іс жүргізу тетіктерін енгізудің қажеттілігі негізделеді.

Кілт сөздер: киберқылмыстылық, ақпараттық қауіпсіздік саласындағы қылмыстар, электрондық дәлелдеме, қылмыстық құқықбұзушылықтар, ақпараттандыру және байланыс саласы, интернет-алаяқтық, қылмыстық жауаптылық.

LEGAL SAFEGUARDS FOR CITIZENS AFFECTED BY INTERNET FRAUD

M.Z. Omarbekova*
Supreme Court of the RK, Astana, Kazakhstan
*e-mail: madeniyeto@mail.ru

M.Z. Omarbekova – Judge of the Supreme Court of the Republic of Kazakhstan, PhD in Law, Professor at the Academy of Justice under the Supreme Judicial Council of the Republic of Kazakhstan; Astana, Republic of Kazakhstan; ORCID ID: https://orcid.org/0009-0007-1323-9597; e-mail: madeniyeto@mail.ru

Abstract. The article examines the improvement of criminal procedure regulation in the Republic of Kazakhstan in the context of the growth of cybercrime and the development of international cooperation in this field. It analyses the key strategic documents in the sphere of cybersecurity (the Cybersecurity Concept "Cyber Shield of Kazakhstan" and the Concept for Digital Transformation, Development of ICT and Cybersecurity for 2023–2029), as well as the significance of Kazakhstan's accession to the Budapest Convention on Cybercrime and the UN Convention on Cybercrime for facilitating cross-border access to electronic evidence and ensuring prompt international cooperation. The article argues that the current criminal procedure legislation provides only fragmentary regulation of electronic documents and computer information, which does not meet the practical needs of detecting and investigating cybercrimes. It substantiates the necessity of legally enshrining the concept of electronic evidence, its classification depending on the place of storage, and the introduction of special procedural mechanisms for obtaining, preserving, seizing and using such evidence in criminal proceedings, taking into account relevant international standards.

Keywords: cybercrime, information security offences, electronic evidence, criminal offences, ICT sector, internet fraud, criminal liability.

Введение. Актуальность исследования обусловлена стремительным развитием цифровых технологий, электронных информационных систем и телекоммуникационных сетей, что, наряду с положительными результатами цифровизации, привело к активному распространению киберпреступности.

Лица, совершающие киберпреступления, используют специальные технические знания и современные информационные технологии для получения незаконного доступа к банковским счетам и персональным данным граждан. Подобные действия совершаются с целью хищения денежных средств, вымогательства, мошенничества, преследования, психологического давления, а также проведения кибератак на организации посредством вредоносного программного обеспечения и иных цифровых инструментов.

Одной из наиболее распространённых и динамично развивающихся угроз в современной цифровой среде является незаконное завладение имуществом или приобретение права на него путём обмана либо злоупотребления доверием пользователей информационных

систем или сети Интернет. В законодательстве Республики Казахстан подобные деяния квалифицируются как интернет-мошенничество в соответствии с п. 4 ч. 2 ст. 190 Уголовный кодекс Республики Казахстан (Уголовный кодекс РК, 2014).

Под интернет-мошенничеством понимаются противоправные действия лица, направленные на незаконное завладение имуществом либо правом на имущество пользователей информационных систем посредством использования информационных технологий. Такие действия могут осуществляться через компьютерные программы, интернет-ресурсы, мобильные устройства и другие цифровые средства, включая размещение заведомо ложной информации или использование вредоносных программ с целью введения пользователей в заблуждение и последующего получения их денежных средств через интернет-банкинг, электронные кошельки и иные финансовые сервисы. Данное понимание отражено в практике применения законодательства о мошенничестве.

Особенности цифровой среды позволяют преступникам взаимодействовать одновременно с большим количеством пользователей, скрывать своё фактическое местонахождение, применять поддельные интернет-ресурсы, фальшивые аккаунты и вредоносные программы. Всё это значительно усложняет выявление подобных преступлений и способствует росту количества противоправных действий, связанных с хищением денежных средств и персональных данных граждан.

Статистические сведения подтверждают устойчивую тенденцию роста интернет-мошенничества. Так, в 2023 году по п. 4 ч. 2 ст. 190 УК Республики Казахстан было рассмотрено 159 уголовных дел, из которых по 125 делам вынесены обвинительные приговоры, а 16 дел прекращены. Общая сумма причинённого ущерба составила 33 951 085 тенге.

В 2024 году количество рассмотренных уголовных дел увеличилось до 299, при этом обвинительные приговоры были вынесены по 208 делам. Общий размер ущерба составил 82 838 370 тенге.

За первые девять месяцев 2025 года было рассмотрено 284 уголовных дела, по 210 из которых вынесены приговоры. Кроме того, 47 дел были прекращены, а 19 возвращены прокурору. Общая сумма причинённого ущерба достигла 546 897 508 тенге. Указанные статистические данные получены из автоматизированной судебной системы Төрелік (Төрелік).

Представленные данные свидетельствуют о значительном увеличении количества интернет-мошенничеств и подтверждают актуальность дальнейшего совершенствования правовых механизмов противодействия подобным преступлениям.

Материалы и методы. В процессе исследования были изучены материалы следственной и судебной практики, а также проведён анализ действующих нормативных правовых актов и научных источников. При толковании норм уголовного и уголовно-процессуального законодательства применялась комплексная методология исследования.

В работе использовались как общенаучные, так и специальные методы научного познания. К их числу относятся методы анализа и синтеза, индукции и дедукции, обобщения, системно-структурный и формально-юридический подходы, а также логический и сравнительно-правовой методы исследования.

Обсуждение. На практике значительная часть преступлений в сфере информационно-коммуникационных технологий связана с дистанционным хищением денежных средств граждан посредством сети Интернет и мобильной связи. Подобные преступления нередко характеризуются бесконтактным способом совершения и отсутствием непосредственного взаимодействия между преступником и потерпевшим.

В судебной практике встречаются различные примеры подобных преступлений. Так, гражданин Е., ранее неоднократно привлекавшийся к уголовной ответственности за мошенничество, был признан виновным в совершении интернет-мошенничества и осуждён к лишению свободы сроком более пяти лет. Судом было установлено, что, находясь в исправительном учреждении, он получил доступ к мобильному телефону и зарегистрировался

в мессенджере WhatsApp.

Используя социальную сеть Instagram, злоумышленник обнаружил видеозапись с воинской присягой и решил использовать её для реализации преступного умысла. Он зарегистрировался на интернет-ресурсе 1xBet, через который впоследствии осуществлял вывод денежных средств, полученных незаконным путём (Төрелік).

Представляясь военнослужащим и вводя граждан в заблуждение, преступник обращался к пользователям сети с просьбой о финансовой помощи, ссылаясь на сложное материальное положение. Потерпевшие, не подозревая о преступных намерениях, переводили денежные средства на указанные им реквизиты.

Как показывает международная практика, наиболее часто жертвами интернет-мошенников становятся социально уязвимые категории населения, включая пожилых людей, несовершеннолетних, а также граждан, не обладающих достаточными навыками использования современных цифровых устройств.

К числу наиболее распространённых способов совершения интернет-мошенничества относятся различные схемы хищения денежных средств с использованием банковских карт и онлайн-платежей. Нередко злоумышленники звонят гражданам, представляясь сотрудниками банковских организаций, и сообщают ложную информацию о якобы совершённых операциях по банковскому счёту либо угрозе блокировки карты. В результате потерпевшие под влиянием обмана переводят денежные средства на указанные мошенниками счета (Абеуов, 2024: 12).

Другим распространённым способом является использование фишинговых интернет-ресурсов. В таких случаях преступники создают сайты-двойники известных сервисов и предлагают пользователям ввести данные банковской карты, включая номер, срок действия и CVV-код. Получив указанную информацию, злоумышленники получают доступ к финансовым средствам потерпевшего.

Ещё одним способом совершения преступления является распространение вредоносного программного обеспечения. Пользователю направляется электронное сообщение со ссылкой либо предложением установить программу, которая на самом деле содержит вирус. После установки подобного программного обеспечения преступники получают удалённый доступ к устройству и могут осуществлять финансовые операции без ведома владельца.

Также распространённой схемой является взлом аккаунтов пользователей в социальных сетях. После получения доступа к аккаунту злоумышленники рассылают сообщения от имени владельца страницы с просьбой одолжить денежные средства либо оказать финансовую помощь.

Кроме того, преступники нередко используют интернет-площадки объявлений, такие как OLX и Kolesa.kz. Под видом покупателей или продавцов они направляют пользователям ссылки на поддельные сайты, внешне похожие на официальный ресурс Казпочта. Вводя свои персональные данные и банковскую информацию на подобных страницах, потерпевшие фактически передают доступ к своим денежным средствам мошенникам.

Следует отметить, что перечисленные способы совершения преступлений не являются исчерпывающими. На практике встречаются также так называемые брачные мошенничества, предложения участия в фиктивных инвестиционных проектах, а также сообщения о несуществующих наследствах.

Несмотря на разнообразие применяемых схем, большинство подобных преступлений основано на использовании методов социальной инженерии. Преступники стремятся установить доверительные отношения с потенциальной жертвой, воздействуют на её эмоциональное состояние и побуждают совершить действия, приводящие к передаче денежных средств (Альсеитов, Идрисов, Омарбекова, 2022).

В целом уголовно-правовая характеристика интернет-мошенничества во многом совпадает с характеристикой традиционного мошенничества, поскольку общественная опасность и основные признаки состава преступления остаются аналогичными. Основное отличие заключается в том, что преступление совершается с использованием информационно-коммуникационных технологий.

При хищении, совершаемом путем интернет-мошенничества, ложные сведения об определенных обстоятельствах, дающих право на получение имущества, не просто сообщаются, а подтверждаются обманными действиями, направленными на то, чтобы ввести в заблуждение лицо, во владении или ведении которого находится имущество, и убедить его в необходимости передать это имущество виновному, либо иные сведения, способствующие этому.

Любой обман должен считаться мошенническим, если он направлен на возбуждение у потерпевшего (пользователя информационной системы) желания или согласия передать мошеннику имущество или право на имущество (к примеру, СМС-код подтверждение).

При этом обязательным условием рассматриваемого мошенничества является то, что обман выступает как способ воздействия на сознание потерпевшего (пользователя информационной системы), средство внушения, убеждения, что распоряжение имуществом осуществляется им на основании закона или иных правовых актов в его собственных интересах.

Другим способом интернет-мошенничества закон называет злоупотребление доверием, при котором виновный в целях незаконного завладения имуществом или правом на имущество использует специальные полномочия виновного или его личные доверительные отношения, сложившиеся между ним и собственником или иным владельцем этого имущества, совершает его обман либо вводит в заблуждение.

Отличительной особенностью объективной стороны интернет-мошенничества является то, что потерпевший, находясь в состоянии добросовестного заблуждения, добровольно передает имущество или предоставляет преступнику право на имущество. Вследствие этого переход имущества обычно выглядит внешне как соглашение сторон, сделка. Однако такая сделка юридически незаконна, так как совершена в ущерб воле потерпевшего.

К примеру, приговором суда гр. С. осужден по ст. 190 ч. 2 п. 4) УК к 2 годам ограничения свободы с установлением пробационного контроля за то, что 6 апреля 2023 года, находясь в ТД «Астана», встретил ранее знакомую гр. А., у которой попросил мобильный телефон для осуществления звонка. Гр. А., не подозревая о преступных намерениях осужденного, передала ему мобильный телефон марки «Honor X6». После чего гр. С. с целью совершения мошенничества, используя персональные данные потерпевшей, с мобильного телефона гр. А. оформил онлайн-кредиты в АО «Kaspi Bank» на имя гр. А. на общую сумму 939 980 тенге, а именно: 6 апреля 2023 года на сумму 269 990 тенге, 6 апреля 2023 года - 669 990 тенге (Төрелік).

Интернет-мошенничество совершается с прямым умыслом и корыстной целью и причиняет реальный ущерб.

Очевидно, что борьба с интернет-мошенничеством является международной проблемой. Каждая страна имеет свои законы и институты, которые способствуют борьбе с киберпреступностью, в том числе и с интернет-мошенничеством. Большинство стран сформировали специальные органы по борьбе с киберпреступлениями, разрабатывают и осуществляют меры, направленные на усиление борьбы с киберпреступностью в международном масштабе.

Анализ законодательства других стран показывает, что в некоторых уголовных кодексах имеется самостоятельная статья, устанавливающая ответственность за интернет-мошенничество. К примеру, в Уголовном кодексе Российской Федерации с 2012 года введена ст. 169.6 УК, предусматривающая ответственность за мошенничество в сфере компьютерной информации, то есть хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей (Уголовный кодекс РФ, 1996).

Вместе с тем, в диспозиции указанной статьи не указано, что чужое имущество похищается путем обмана или злоупотребления доверием, а предусмотрено, что мошенничество совершается путем использования компьютерной информации.

Уголовная ответственность за хищение путем использования информационных

технологий также предусмотрена ст. 212 УК Республики Беларусь.

Уголовное законодательство Германии, как и в российском уголовном законе, содержит общую норму о мошенничестве (§ 263 УК ФРГ) и специальную норму о компьютерном мошенничестве (§ 263а) УК ФРГ), которые считаются преступлениями против собственности.

В США, Англии и Австралии интернет–мошенничество отнесено к преступлениям обманного характера.

В Республике Казахстан, в целях обеспечения комплексной защиты объектов информатизации, электронных информационных систем, телекоммуникационных сетей, а также безопасного функционирования и использования цифровой инфраструктуры, принят ряд ключевых стратегических документов в сфере кибербезопасности, в том числе Концепция кибербезопасности («Киберщит Казахстана»), утвержденная постановлением Правительства Республики Казахстан от 30 июня 2017 года № 407 и Концепция цифровой трансформации, развития отрасли информационно-коммуникационных технологий и кибербезопасности на 2023–2029 годы, утвержденная постановлением Правительства Республики Казахстан от 28 марта 2023 года № 269.

Для эффективного противодействия киберпреступности, в том числе интернет-мошенничеству, помимо адекватного отечественного законодательства необходимо укреплять и развивать международное сотрудничество по оказанию правовой помощи по делам о киберпреступлениях, при расследовании которых важное значение приобретают электронные доказательства.

В 2023 году Республике Казахстан было предложено присоединиться к Будапештской Конвенции о компьютерных преступлениях. В этой связи в настоящее время проводится работа по приведению Парламентом отечественного законодательства в соответствии со стандартами данной Конвенции. В свою очередь, Будапештская Конвенция и Второй дополнительный протокол к ней предусматривают упрощенные процедуры, такие как прямое сотрудничество с крупнейшими мировыми поставщиками услуг и использование круглосуточных сетей формата 24/7.

27 октября 2025 года Республика Казахстан присоединилась к Конвенции Организации Объединенных Наций против киберпреступности, принятой Генеральной Ассамблеей Организации Объединенных Наций 24 декабря 2024 года. Конвекция направлена на 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.

Присоединение к Конвенции ООН позволит Республике Казахстан оперативно обмениваться электронными доказательствами с другими странами; эффективнее взаимодействовать при расследовании трансграничных киберпреступлений: надежно защищать граждан от интернет-мошенничества, кибератак и других угроз в цифровом пространстве (Конвенция ООН против киберпреступности, 2024).

Указанные две Конвенции против киберпреступности дополняют друг друга и предоставляют уникальную возможность создать оперативную и эффективную систему международного сотрудничества в борьбе с киберпреступностью, содействия трансграничному доступу к электронным доказательствам.

Заключение. В связи с присоединением к международным договорам и ростом киберпреступности возникает необходимость реформирования отечественного уголовно-процессуального законодательства.

Раскрытие киберпреступности и их расследование традиционными способами и методами является недостаточным, так как требует специальных познаний в области информатизации и связи, новых технических приемов, методов и процессуальных полномочий по сбору, раскрытию, сохранности, выемке и предоставлению электронных доказательств.

Электронные доказательства – это хранимая или пересылаемая цифровая информация: электронные документы, фотоснимки, электронные письма, аудио, видеозаписи, программные продукты и иные цифровые данные, имеющие доказательственное значение для дела. В

зависимости от места хранения электронные доказательства можно разделить на локальные (компьютеры, телефоны, SIM-карты, флэш-накопители, карты памяти, банковские карты, видеорегистраторы, сетевые накопители) и удаленные (облачные) (облачные хранилища, например, Google Drive, Яндекс.Диск, Dropbox, web-сайты, удаленные серверы) (Convention, 2001).

В УПК РК дано понятие электронного документа в п. 15) ст. 7, как документа, в котором информация представлена в электронно-цифровой форме и удостоверена посредством электронной цифровой подписи и в ч. 3 ст. 120 УПК РК к документам, кроме понятия в общепринятом смысле, то есть зафиксированным в письменной форме, также относятся материалы, содержащие компьютерную информацию, фото и киносъемки, звуко-, видеозаписи (Уголовно-процессуальный кодекс РК, 2014).

Таким образом, понятие электронных доказательств, их получение и использование в уголовном процессе являются вопросами, требующими включения в уголовно-процессуальное законодательство.

Литература

Абеуов, 2024 - Абеуов Д.А. Противодействие киберугрозам в Республике Казахстан: проблемы и пути решения на современном этапе // «Хабаршы-Вестник» Карагандинской академии МВД РК им. Б. Бейсенова. — 2024. — № 4 (86). — С. 10-13.
Альсеитов, Идрисов, Омарбекова, 2022 - Альсеитов К.Г., Идрисов Р.Д., Омарбекова М.Ж. и др. Практическое руководство по выявлению, расследованию и судебному рассмотрению преступлений, совершаемых с использованием сети Интернет и электронных информационных ресурсов. — Нур Султан: «АВА», 2022. -194 с.
Конвенция ООН против киберпреступности, 2024 - Конвенция Организации Объединенных Наций против киберпреступности; укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационнокоммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям / Принята резолюцией 79/243 Генеральной Ассамблеей от 24 декабря 2024 года. - URL: https://www.un.org/ru/documents/treaty/A-RES-79-243 (дата обращения 02.12.2025)
Нормативное постановление, 2017 - Нормативное постановление Верховного Суда Республики Казахстан от 29 июня 2017 года № 6 «О судебной практике по делам о мошенничестве». Сборник. – Алматы: Юрист, 2021. – 660 с.
Төрелік - Автоматизированная информационно-аналитическая система «Төрелік».
Уголовный кодекс РК, 2014 - Уголовный кодекс Республики Казахстан от 3 июля 2014 года. № 226-V ЗРК. [Электрон. ресурс] - URL: https://adilet.zan.kz/rus/docs/K1400000226 (дата обращения 02.12.2025)
Уголовный кодекс РФ, 1996 - Уголовный кодекс Российской Федерации с постатейными разъяснениями Пленума Верховного Суда Российской Федерации. - Москва: ООО «Проспект», 2022. – 816 с.
Уголовно-процессуальный кодекс РК, 2014 - Уголовно-процессуальный кодекс Республики Казахстан от 4 июля 2014 года № 231-V ЗРК. - URL: https://adilet.zan.kz/rus/docs/K1400000231 (дата обращения 02.12.2025)
Convention, 2001 - Convention on Computer Information Crime (ETS N 185). (Concluded in Budapest on 11/23/2001). - URL: https://rm.coe.int/1680081580. (дата обращения 05.12.2025).

References

Abeuov, 2024 - Abeuov D.A. Protivodejstvie kiberugrozam v Respublike Kazahstan: problemy i puti resheniya na sovremennom etape [Countering cyber threats in the Republic of Kazakhstan: problems and solutions at the present stage] // «Habarshy-Vestnik» Karagandinskoj akademii MVD RK im. B. Bejsenova. — 2024. — № 4 (86). — S. 10-13. [Russ.]
Al'seitov, Idrisov, Omarbekova, 2022 - Al'seitov K.G., Idrisov R.D., Omarbekova M.Zh. i dr. Prakticheskoe rukovodstvo po vyyavleniyu, rassledovaniyu i sudebnomu rassmotreniyu prestuplenij, sovershaemyh s ispol'zovaniem seti Internet i elektronnyh informacionnyh resursov [A practical guide to the detection, investigation and prosecution of crimes committed using the Internet and electronic information resources]. — Nur Sultan: «ABA», 2022. -194 s. [Russ.]
Convention, 2001 - Convention on Computer Information Crime (ETS N 185). (Concluded in Budapest on 11/23/2001). - URL: https://rm.coe.int/1680081580. (data obrashcheniya 05.12.2025). [Eng]
Konvenciya OON protiv kiberprestupnosti, 2024 - Konvenciya Organizacii Ob"edinennyh Nacij protiv kiberprestupnosti; ukreplenie mezhdunarodnogo sotrudnichestva v bor'be s opredelennymi prestupleniyami, sovershaemymi s ispol'zovaniem informacionnokommunikacionnyh sistem, i v obmene dokazatel'stvami v elektronnoj forme, otnosyashchimisya k ser'eznym prestupleniyam / Prinyata rezolyuciej 79/243 General'noj Assambleej ot 24 dekabrya 2024 goda [United Nations Convention against Cybercrime]. - URL: https://www.un.org/ru/documents/treaty/A-RES-79-243 (data obrashcheniya 02.12.2025) [Russ.]
Normativnoe postanovlenie, 2017 - Normativnoe postanovlenie Verhovnogo Suda Respubliki Kazahstan ot 29 iyunya 2017 goda № 6 «O sudebnoj praktike po delam o moshennichestve» [On judicial practice in fraud cases]. Sbornik. – Almaty: YUrist, 2021. – 660 s. [Russ.]
Tørelik - Avtomatizirovannaya informacionno-analiticheskaya Sistema [Automated information and analytical system] «Tørelik». [Russ.]
Ugolovnyj kodeks RF, 1996 - Ugolovnyj kodeks Rossijskoj Federacii s postatejnymi raz"yasneniyami Plenuma Verhovnogo Suda Rossijskoj Federacii [Criminal Code of the Russian Federation]. - Moskva: OOO «Prospekt», 2022. – 816 s. [Russ.]
Ugolovno-processual'nyj kodeks RK, 2014 - Ugolovno-processual'nyj Kodeks Respubliki Kazahstan ot 4 iyulya 2014 goda № 231-V ZRK [Criminal Procedure Code of the Republic of Kazakhstan]. - URL: https://adilet.zan.kz/rus/docs/K1400000231 (data obrashcheniya 02.12.2025) [Russ.]
Ugolovnyj kodeks RK, 2014 - Ugolovnyj kodeks RK, 2014 - Ugolovnyj kodeks Respubliki Kazahstan ot 3 iyulya 2014 goda [Criminal Code of the Republic of Kazakhstan]. № 226-V ZRK. - URL: https://adilet.zan.kz/rus/docs/K1400000226 (data obrashcheniya 02.12.2025) [Russ.]