



Т.С. Салкебаев¹, Р.К. Джиембаев²

¹Қарағандинский университет Казпотребсоюза, г. Караганда, Республика Казахстан

²Қарағандинская академия Министерства внутренних дел Республики Казахстан имени Б. Бейсенова, г. Караганда, Республика Казахстан

ПРОБЛЕМЫ РАЗГРАНИЧЕНИЯ ИНТЕРНЕТ-МОШЕННИЧЕСТВА И КИБЕРПРЕСТУПНОСТИ В КОНТЕКСТЕ УГОЛОВНО-ПРАВОВОЙ ЗАЩИТЫ СОБСТВЕННОСТИ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация. В настоящей статье исследуются проблемы разграничения интернет-мошенничества и киберпреступности в условиях цифровой трансформации общественных отношений. Цель исследования заключается в разработке уголовно-правовых критериев их дифференциации на основе анализа объекта посягательства и функциональной роли информационной системы в механизме преступления. Обосновано, что киберпреступность охватывает деяния, в которых информационные системы выступают непосредственным объектом уголовно-правовой охраны, тогда как интернет-мошенничество представляет собой посягательство на собственность, при котором цифровые технологии используются как инструмент реализации обмана. Сформулирован вывод о том, что дистанционный способ воздействия на потерпевшего не образует признаков интернет-мошенничества при отсутствии использования ресурсов информационной системы для осуществления обмана. Полученные результаты имеют значение для обеспечения единообразия квалификации и уточнения пределов уголовно-правовой охраны имущественных и информационных отношений.

Ключевые слова: интернет-мошенничество; киберпреступность; уголовное право; правособственности; информационная безопасность; цифровая трансформация; недвижимое имущество; мошеннические схемы; уголовная ответственность.

Т.С. Салкебаев¹, Р.К. Джиембаев²

¹Қазтұтынуодағы Қарағанды университеті, Қарағанды қ., Қазақстан Республикасы

²Қазақстан Республикасы Ішкі істер министрлігінің Б. Бейсенов атындағы Қарағанды академиясы, Қарағанды қ., Қазақстан Республикасы

МҮЛІКТІ ҚЫЛМЫСТЫҚ-ҚҰҚЫҚТЫҚ ҚОРҒАУ ЖӘНЕ АҚПАРАТТЫҚ ҚАУІПСІЗДІК КОНТЕКСТІНДЕГІ ИНТЕРНЕТ-АЛАЯҚТЫҚ ПЕН КИБЕРҚЫЛМЫСТЫ АЖЫРАТУ МӘСЕЛЕЛЕРІ

Аннотация. Мақалада қоғамдық қатынастардың цифрлық трансформациясы жағдайында интернет-алаяқтық пен киберқылмысты ажырату мәселелері зерттеледі. Зерттеудің мақсаты – құқық бұзушылық объектісінің сипаты мен қылмысты жасау механизміндегі ақпараттық жүйенің функционалдық рөлін негізге ала отырып, оларды қылмыстық-құқықтық тұрғыдан саралау өлшемдерін әзірлеу. Қылмыстық қол сұғушылықтың тікелей объектісін және ақпараттық жүйенің қылмыстық әрекеттегі орнын айқындауға негізделген ажырату критерийлері ұсынылады. Ақпараттық жүйелер мен ақпараттық қауіпсіздік саласындағы қатынастар тікелей қылмыстық қол сұғушылық объектісі болып табылатын әрекеттер киберқылмыс ретінде қарастырылуы тиіс екендігі негізделеді, ал интернет-алаяқтық цифрлық технологиялар алдау құралы ретінде пайдаланылатын меншікке қарсы дәстүрлі қылмыстың нысаны ретінде бағаланады. Жәбірленушіге қашықтан ықпал ету тәсілі, егер алдау ақпараттық жүйе ресурстарын пайдалану арқылы жүзеге асырылмаса, өздігінен интернет-алаяқтық белгілерін құрамайтыны туралы қорытынды жасалады. Алынған нәтижелер қылмыстық-құқықтық саралаудың бірізділігін қамтамасыз ету және мүліктік әрі ақпараттық қатынастарды қорғау шектерін нақтылау үшін практикалық маңызға ие.

Түйінді сөздер: интернет-алаяқтық; киберқылмыс; қылмыстық құқық; меншік құқығы; ақпараттық



қауіпсіздік; цифрлық трансформация; жылжымайтын мүлік; алаяқтық схемалар; қылмыстық жауаптылық.

T.S. Salkebaev¹, R.K. Dzhiembaev²

¹*Karaganda University of Kazpotreboysuz, Karaganda, the Republic of Kazakhstan*

²*Karaganda Academy of the Ministry of Internal Affairs of the Republic of Kazakhstan named after B. Beisenov, Karaganda, the Republic of Kazakhstan*

PROBLEMS OF DIFFERENTIATING BETWEEN INTERNET FRAUD AND CYBERCRIME IN THE CONTEXT OF CRIMINAL LAW PROTECTION OF PROPERTY AND INFORMATION SECURITY

Abstract. The article examines the problem of differentiating between Internet fraud and cybercrime in the context of the digital transformation of social relations. The purpose of the study is to develop criminal law criteria for distinguishing these offenses based on the nature of the object of encroachment and the functional role of information systems in the mechanism of the crime. The paper proposes criteria for differentiation grounded in the identification of the direct object of criminal encroachment and the role of information systems in the commission of the offense. It is substantiated that cybercrime should encompass acts in which information systems and relations in the field of information security constitute the direct object of criminal protection, whereas Internet fraud represents a form of traditional property infringement in which digital technologies are used as an instrument of deception. It is concluded that a remote method of influencing the victim does not in itself constitute Internet fraud unless the deception is carried out through the use of information system resources. The results are significant for ensuring consistent legal qualification and for clarifying the limits of criminal law protection of property and information relations.

Keywords: Internet fraud; cybercrime; criminal law; property rights; information security; digital transformation; real estate; fraudulent schemes; criminal liability.

DOI: 10.52425/25187252_2026_39_106

Введение. Современные цифровые технологии, проникая во все сферы общественной жизни, создают не только новые возможности, но и формируют принципиально иные угрозы криминального характера. Особую актуальность приобретает проблема эволюции мошеннических схем, реализуемых в виртуальном пространстве, где традиционные критерии уголовно-правовой квалификации зачастую демонстрируют свою недостаточную эффективность. В этой связи в научной доктрине уголовного права все чаще поднимается дискуссия о необходимости строгого концептуального разделения таких категорий, как «киберпреступность» и «интернет-мошенничество», поскольку их терминологическая и содержательная контаминация приводит к существенным сложностям в правоприменительной практике. Смешение указанных понятий порождает не только проблемы процессуального характера, но и создает доктринальную неопре-

деленность в вопросе защиты охраняемых законом социальных ценностей. Проблема квалификации мошеннических действий, предметом которых выступает недвижимое имущество, заслуживает особого внимания, учитывая специфику их совершения с применением дистанционных коммуникационных технологий. Подобные преступления требуют тщательного анализа не только с точки зрения объективной стороны состава, но и с позиции уточнения непосредственного объекта уголовно-правовой охраны.

Материалы и методы. В исследовании применен комплексный методологический подход, основанный на использовании общенаучных методов анализа, синтеза, индукции и дедукции, а также частнонаучных методов, среди которых сравнительно-правовой, нормативный, формально-юридический и статистический методы.

Материалами исследования послужили нормы уголовного законодательства



Республики Казахстан (далее – РК), иные нормативно-правовые акты и официальные документы, регулирующие вопросы уголовно-правовой охраны собственности и информационной безопасности, а также правоприменительная практика и статистические данные уполномоченных государственных органов. Существенное значение имели научные труды зарубежных и отечественных авторов, посвященные проблемам киберпреступности, интернет-мошенничества и трансформации традиционных форм хищений в цифровой среде. При анализе учитывались предложения исследователей, результаты изучения нормативных актов и статистических данных, что позволило выявить проблемы разграничения интернет-мошенничества и киберпреступности, определить направления совершенствования уголовно-правовой защиты имущественных прав и информационной безопасности.

Результаты, обсуждение. Темпы технологического развития человечества к настоящему времени требуют более четкого разграничения понятия «киберпреступность» от иных разновидностей преступлений, совершаемых с использованием информационных технологий, к которым относится и интернет-мошенничество. Учитывая объем элементов цифрового пространства, включенного в жизнь современного человека, относить все криминальные инциденты, совершаемые посредством информационных систем, к киберпреступности (т.е. так называемой «преступности в сфере высоких технологий») будет необоснованным. В этом смысле более предпочтительным представляется четкое разграничение собственно преступления в сфере информационного пространства (в различных вариантах наименования соответствующего объекта) от преступлений, в механизме которых используются ресурсы информационных систем.

Схожая позиция высказывается и в зарубежной уголовно-правовой доктрине, в рамках которой проводится разграничение

между преступлениями, невозможными вне цифровой среды, и традиционными составами, лишь совершаемыми с использованием информационных технологий [1]. Зарубежными исследователями подчеркивается, что использование цифровых технологий само по себе не формирует самостоятельный вид преступности и не подменяет традиционные уголовно-правовые конструкции [2].

В этом контексте типология интернет-мошенничества имеет исключительно эмпирический (констатируемый) или даже эвристический (в случае появления новых форм) метод формирования, поскольку в уголовно-правовом аспекте значение имеет только факт обмана и злоупотребления доверием пользователя информационной сети. Авторы исследований, к примеру, отмечают, что наиболее распространенными видами преступлений в сети Интернет, связанных с хищениями, являются так называемые «нигерийские письма» [3], фишинг [4] и вишинг [5].

Европол¹ среди наиболее распространенных форм интернет-преступлений отмечает мошенничество в сфере онлайн-платежей, инвестиционное мошенничество, а также схемы компрометации корпоративной электронной переписки (Business Email Compromise). Указанные деяния отнесены к категории «cyber-enabled crimes», поскольку цифровая инфраструктура используется в них как инструмент реализации преступного замысла. В отличие от этого, неправомерный доступ к информационным системам, вмешательство в их функционирование и иные посягательства на цифровую инфраструктуру рассматриваются как самостоятельные киберзависимые преступления (cyber-dependent offences), объективно невозможные вне цифровой среды.

Данная классификация подтверждает, что разграничение интернет-мошенничества и киберпреступности должно основываться на характере непосредственного объекта посягательства и функциональной роли информационной системы в механизме совершения деяния, а не на технической

¹ Internet Organised Crime Threat Assessment (IOCTA) 2024. The Hague: Europol, 2024 [Электронный ресурс] – Режим доступа: <https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024> (дата обращения: 25.02.2026).



форме либо сложности используемой схемы. Типология мошеннических приемов имеет вспомогательное значение и не предопределяет уголовно-правовую квалификацию. Законодательная дифференциация интернет-мошенничества оправдана лишь постольку, поскольку она связана с признаками, повышающими степень общественной опасности деяния.

Проблема классификации интернет-мошенничества непосредственно связана с вопросом об объекте преступления и предмете уголовно-правовой охраны. В связи с постоянным расширением способов и форм совершения мошенничества в сети возникает необходимость уточнения правовых подходов к определению того, какие именно общественные отношения и ценности подлежат защите.

Категория объекта преступления в целом является одной из самых неоднозначных в теории уголовного права. Причем, как указывает В. Анисимов, понятие «собственность» как самостоятельный объект уголовно-правовой охраны неизбежно подвергается и будет подвергаться пересмотру за счет включения в структуру предмета преступления все новых видов имущества, появляющихся по причине научно-технического развития. При этом автор полагает, что информация является специфическим предметом, на который распространяется право собственности, по причине чего аргументирует целесообразность перенесения всех «компьютерных» преступлений в главу преступлений против собственности [6, 16 стр.]. Мы не в полной мере согласны с данным мнением автора (хотя динамика развития правового поля и теоретической мысли может привести к различным трансформациям). Вместе с тем нельзя отрицать фактор возрастания значимости информации и гарантий ее сохранности в современном обществе, где виртуализация персональных данных граждан во многом и приводит к детерминации интернет-мошенничества. В этом смысле будет справедливым утверждение, что в контексте интернет-мошенничества информационная

безопасность выступает в качестве дополнительного объекта преступления.

Право собственности как объект посягательства при всех видах мошенничества, в т.ч. интернет-мошенничестве, лидирует по уязвимости в общей структуре объектов уголовных правонарушений. В данном случае речь идет не об относительной оценке качественных показателей вреда от тех или иных посягательств. Здесь следует исходить исключительно из подтверждаемого статистическими данными факта, что посягательства на собственность преобладают в общей структуре преступности. Кроме того, сопоставление степени вреда различных по характеру уголовных правонарушений представляется затруднительным и даже некорректным (например, вреда от корыстных и насильственных преступлений). Явное лидерство корыстной мотивации в оценке параметров современной преступности во многом предопределяет и тот факт, что именно уголовные правонарушения против собственности являются наиболее склонными к повторности и рецидивизму [7, 62 стр.].

Традиционно в рамках правоотношений собственника принято понимать единство трех основных полномочий: права владения, пользования и распоряжения. Авторы тематических исследований иногда предлагают выделить дополнительные полномочия, в частности, полномочия в плане решения вопроса о том, допускать или не допускать к своему имуществу других лиц [8, 16 стр.]. Если речь будет идти о праве собственности на обективированные вещи (недвижимость, денежные средства, земельный участок и т.д.), то здесь полномочия по «недопуску» к своему имуществу иных лиц имеет вполне конкретное воплощение за счет тех или иных способов охраны принадлежащего имущества. Перевод значительного количества платежных и иных операций в режим онлайн большинством граждан способствует тому, что их волевое решение на «допуск» к своему имуществу других лиц претерпевает определенную трансформацию. Возникает



неизбежная зависимость от исправности информационно-коммуникационных систем, уровня защиты банковских приложений, добросовестности поставщиков соответствующих услуг и других обстоятельств, в результате на которые у собственника весьма ограниченные возможности.

Рост количества случаев интернет-мошенничества сопровождается увеличением имущественного вреда, причиняемого собственникам. В криминологии часто используется термин «цена преступности», который охватывает совокупность негативных последствий для потерпевших, общества и правоохранительной системы. Противодействие таким посягательствам требует дополнительных финансовых и организационных ресурсов. Кроме того, распространение подобных преступлений способно снижать экономическую привлекательность региона, усиливая инвестиционные и финансовые риски. [9, 131 стр.].

Исходя из данных официальной статистики Комитета по правовой статистике и специальным учетам Генеральной прокуратуры РК, был только 1 случай регистрации мошенничества в отношении недвижимого имущества (в рамках статданных отсутствует возможность установить, было ли это «простое» или интернет-мошенничество) в 2022 году. При этом дела по 4-ем мошенничествам в отношении недвижимого имущества находились в производстве. Особые свойства недвижимого имущества, независимо от разновидности мошеннических действий, требуют, на наш взгляд, более тщательного учета данного признака. Здесь дело не столько в значительном стоимостном выражении похищенного имущества, сколько в том обстоятельстве, что недвижимость представляет ценность с точки зрения возможности реализации человеком своих самых насущных потребностей (для проживания его самого и членов его семьи). В целом мошеннические действия в отношении жилых помещений (квартир, домов и т.д.) явно обладают повышенной степенью цинизма со стороны мошенников, особенно когда потерпевшими становятся люди пожилого

возраста, лица с инвалидностью, сироты и т.д.

При этом утрата права на недвижимость, как правило, имеет место именно в рамках мошеннических действий, поскольку только в статье 190 Уголовного кодекса РК (далее – УК РК) указывается на «приобретение права на имущество» (требование права на имущество отмечается также в части 1 статьи 194 УК РК «Вымогательство», однако это гораздо более редкая форма посягательств на собственность, нежели мошенничество). В теории формулировка «право на имущество» вызывает некоторые разногласия. Многие склоняются к тому, что следует ограничиваться термином «имущество», как минимум, по той причине, что право на недвижимое имущество часто является восстановимым [10]. Не останавливаясь подробно на обоснованности данных теоретических споров, тем не менее, следует еще раз сделать акцент на том, что утрата недвижимого имущества (в особенности, жилого помещения) явно должна быть оценена как более общественно опасная форма мошенничества. Даже при условии, что могут быть использованы те или иные механизмы восстановления потерпевшего в правах, этот процесс является достаточно сложным и длительным (в особенности, в случаях, когда недвижимость была приобретена добросовестным покупателем). Особенно критически-негативное значение утрата права на недвижимость будет иметь в ситуациях, когда жилое помещение являлось единственным местом для проживания потерпевшего и его семьи.

В этом смысле мы присоединяемся к позиции исследователей, которые отмечают, что умысел в отношении завладения недвижимостью должен оцениваться как более квалифицированный, даже если в стоимостном выражении ущерб не оказался крупным или особо крупным [11, 157 стр.]. Несмотря на незначительные количественные показатели в статданных по мошенничествам, исследователи обоснованно отмечают риски повышенной уязвимости граждан в случае так называемого «черного риэлторства», поскольку



сложность процедуры оформления права на недвижимость приводит к сложностям его реституции в случае утраты [12, 59 стр.].

Контент-анализ СМИ и иных доступных информационно-коммуникационных ресурсов изобилует информацией относительно совершаемых в Казахстане интернет-мошенничеств. При этом термин «интернет-мошенничество» имеет достаточно произвольную форму применения, поскольку к нему нередко относят и криминальные инциденты, которые в строгом смысле не сопряжены с обманом и злоупотреблением доверием в информационной сети. Так, к примеру, на информационно-коммуникационном ресурсе «Orda.kz» как интернет-мошенничество был представлен случай, имевший место в г. Алматы, в котором мошеннические схемы в отношении четырех потерпевших привели к потере права на недвижимое имущество. При этом мошенники во всех случаях действовали в отношении пенсионеров и по единой схеме: телефонный звонок с сообщением об угрозе относительно банковского счета, убеждение в необходимости срочно реализовать недвижимость для того, чтобы мошенникам не удалось его продать. Дополнительно также обманным путем жертв убеждали в необходимости оформления кредита².

В целом схема мошеннических действий в данном случае является неоригинальной и включает в себя набор уже давно сформировавшихся «штампов»: явное предпочтение в качестве жертв уязвимых лиц (пожилой возраст); психологическое воздействие за счет представления в качестве сотрудника службы безопасности банка (полиции и других структур); введение в заблуждение за счет демонстрации информированности относительно персональных данных потерпевшего и т.д.

Анализ зарубежных открытых источников

показывает, что применение мошеннических схем в отношении пожилых людей не является специфической особенностью отдельных государств, а носит глобальный характер. Так, по данным Federal Bureau of Investigation, в 2023 году совокупный объем финансовых потерь, о которых сообщили граждане США в возрасте старше 60 лет, превысил 3,4 млрд долларов США, что почти на 11% больше по сравнению с предыдущим годом³. Аналогичные выводы содержатся и в материалах National Council on Aging, согласно которым пожилые лица все чаще становятся основными жертвами так называемого «мошенничества с бабушками и дедушками», в т.ч. с использованием технологий искусственного интеллекта и дипфейков, эксплуатирующих эмоциональную уязвимость и чувство тревоги за близких⁴.

Однако имеют ли данные случаи реальное отношение к понятию «интернет-мошенничество»? В соответствии с Законом РК от 24 ноября 2015 года под информационной системой понимается совокупность информационно-коммуникационных технологий, посредством которых осуществляется информационное взаимодействие; при этом анализ данного законодательного акта приводит к выводу, что речь идет только об электронных ресурсах⁵. В приведенном выше примере контактирование мошенников с потерпевшими осуществлялось посредством сотовой связи, которая в соответствии с Законом РК от 5 июля 2004 года относится к электрической связи, предназначенной для обмена информацией⁶. То есть мошенники звонили по аппаратам сотовой связи, деньги передавались непосредственно в руки, кредиты оформлялись путем посещения банков и т.д. — ни в одном звене этой цепочки последовательных мошеннических операций сеть

² Идет спецоперация: как мошенники отбирали у пенсионеров Алматы квартиры и машины [Электронный ресурс] – Режим доступа: <https://orda.kz/ idet-spesoperacija-kak-moshenniki-otbirali-u-pensionerok-almaty-kvartiry-i-mashiny/> (дата обращения: 20.12.2025).

³ Federal Bureau of Investigation. Elder fraud report 2023. – 21 p. [Электронный ресурс] – Режим доступа: https://www.ic3.gov/annualreport/reports/2023_ic3elderfraudreport.pdf (дата обращения: 25.12.2025).

⁴ Understanding Deepfakes: What Older Adults Need to Know [Электронный ресурс] – Режим доступа: <https://www.ncoa.org/article/understanding-deepfakes-what-older-adults-need-to-know/> (дата обращения: 25.12.2025).

⁵ Об информатизации: закон Республики Казахстан от 24 нояб. 2015 г. № 418-V [Электронный ресурс] – Режим доступа: <https://adilet.zan.kz/rus/docs/Z1500000418> (дата обращения: 05.01.2026).

⁶ О связи: закон Республики Казахстан от 5 июля 2004 г. № 567-II [Электронный ресурс] – Режим доступа: https://adilet.zan.kz/rus/docs/Z040000567_ (дата обращения: 05.01.2026).



Интернет фактически не была использована. Безусловно, речь идет о факте завладения теми или иными персональными данными (номера телефонов, ИИН потерпевших и т.п.), однако фактически вести речь об обмане в рамках информационной сети можно лишь с большой долей условности.

Использование «дистанционных» форм воздействия на потерпевших не означает уместность автоматического вменения признаков интернет-мошенничества, если не будет установлено, что виновный реально использовал ресурсы информационной системы для обмана или злоупотребления доверием: разместил ложное объявление; использовал недостоверные сведения о себе при общении в социальных сетях; создавал видимость общения потерпевшего с представителями государственных органов или сотрудников финансовых организаций и т.д. В данном случае следует учитывать, что, во-первых, сама форма коммуникации между людьми в последние годы существенным образом изменилась, и привычным стало дистанционное решение многих вопросов, осуществление переводов, оставление заявок, ознакомление с объявлениями и т.д.; во-вторых, так называемые «холодные контакты» всегда являются более эффективными для реализации криминальных целей, поскольку отсутствует непосредственное (визуально воспринимаемое) взаимодействие между виновным и потерпевшим, в результате которого гораздо больше рисков быть разоблаченным или изменить линию поведения (например, изчувствасо страдания к пожилому или больному человеку).

Заключение. Результаты проведенного исследования свидетельствуют о том, что стремительная цифровая трансформация общественных отношений диктует настоятельную необходимость концептуального разведения терминологических конструкций «киберпреступность» и «интернет-мошенничество». Криминологический анализ позволяет утверждать, что первая из указанных дефиниций должна охватывать исключительно те противоправные деяния,

непосредственным объектом посягательства в которых выступают общественные отношения в сфере информационной безопасности и целостности виртуального пространства. В свою очередь, мошеннические действия, совершаемые с применением цифровых технологий, требуют принципиально иной квалификационной парадигмы, поскольку их основной объект – имущественные права граждан – дополняется производным объектом охраны в виде информационной безопасности личности.

Эмпирические данные демонстрируют, что уголовно-правовая оценка интернет-мошенничества не может основываться исключительно на технической сложности используемых преступных методик. Ключевое значение приобретает установление реального имущественного ущерба и факта нарушения субъективных прав потерпевших. Однако особую криминологическую значимость приобретают мошеннические посягательства на недвижимое имущество, что обусловлено их повышенной социальной опасностью и долгосрочными негативными последствиями для жертв преступления. Наибольший общественный резонанс вызывают преступные схемы, эксплуатирующие уязвимое положение социально незащищенных категорий населения – лиц пенсионного возраста, инвалидов или несовершеннолетних, оставшихся без попечения родителей.

Перспективными направлениями совершенствования законодательства видятся: разработка четких критериев дифференциации интернет-мошенничества от смежных составов преступлений; создание специализированных норм, усиливающих защиту прав собственников недвижимости, а также формирование эффективных правовых механизмов реституции нарушенных имущественных прав. Реализация указанных мер будет способствовать минимизации социально-экономических последствий цифровой преступности, повышению уровня правовой защищенности граждан и стабилизации имущественного оборота в условиях развития информационного общества.



Список использованной литературы:

1. Wall, D.S. Cybercrime: The Transformation of Crime in the Information Age / D.S. Wall. – Polity, 2007 – 288 p.
2. Yar, M. The novelty of cybercrime: An assessment in light of routine activity theory / M. Yar // European Journal of Criminology. – 2005. – Vol. 2. № 4. – Pp. 407-427.
3. Chawki, M. Nigeria tackles advance fee fraud [Электронный ресурс] / M. Chawki // Journal of Information, Law and Technology. – 2009. – No. 1 – Режим доступа: https://go.warwick.ac.uk/jilt/2009_1/chawki (дата обращения: 03.01.2026).
4. R. Dhamija. Why phishing works: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI 2006). – Montreal, Quebec, Canada, 2006. – Pp. 581-590.
5. F. Maggi, Are the con artists back? A preliminary analysis of modern phone frauds: Proceedings of the 10th IEEE International Conference on Computer and Information Technology. – Bradford, West Yorkshire, UK, 2010. – Pp. 824-831.
6. Анисимов, В.Ф. Ответственность за преступления против собственности с признаками хищения: состояние, сущность и проблемы квалификации: дис. ... д-ра юрид. наук / В.Ф. Анисимов. – СПб., 2007. – 381 с.
7. Идрисов, Н.Т. О противодействии рецидивной преступности (на основе практики Следственного комитета Российской Федерации) / Н.Т. Идрисов // Юридический вестник Самарского университета. – 2018. – Т. 4. № 2. – С. 61-64.
8. Камышанский, В.П. Право собственности: пределы и ограничения: монография / В.П. Камышанский. – М.: ЮНИТИ, 2000. – 301 с.
9. Плетнев, Д.А. Институциональные основы прав собственности / Д.А. Плетнев // Вестник Челябинского университета. Серия 8: Экономика. Социология. Социальная работа. – 2006. – № 1. – С. 130-135.
10. Складов, С. Уголовная ответственность за хищение недвижимого имущества [Электронный ресурс] / С. Складов // Российская юстиция. – 2001. – № 6. – Режим доступа: <https://base.garant.ru/987536/> (дата обращения: 03.01.2026).
11. Парфенов, М.Р. К вопросу об особенностях мошенничества в сфере оборота недвижимости с точки зрения необходимости внесения изменений в действующее законодательство / М.Р. Парфенов // Евразийский Союз ученых. – 2014. – № 5-5 (5). – С. 155-159.
12. Плещицкая, Х. Ответственность риелтора: за что и как отвечает риелтор? / Х. Плещицкая // Жилищное право. – 2014. – № 8. – С. 59-60.

References:

1. Wall, D.S. Cybercrime: The Transformation of Crime in the Information Age / D.S. Wall. – Polity, 2007 – 288 p.
2. Yar, M. The novelty of cybercrime: An assessment in light of routine activity theory / M. Yar // European Journal of Criminology. – 2005. – Vol. 2. № 4. – Pp. 407-427.
3. Chawki, M. Nigeria tackles advance fee fraud [Elektronnyj resurs] / M. Chawki // Journal of Information, Law and Technology. – 2009. – No. 1 – Rezhim dostupa: https://go.warwick.ac.uk/jilt/2009_1/chawki (data obrashheniya: 03.01.2026).
4. R. Dhamija. Why phishing works: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI 2006). – Montreal, Quebec, Canada, 2006. – Pp. 581-590.
5. F. Maggi, Are the con artists back? A preliminary analysis of modern phone frauds: Proceedings of the 10th IEEE International Conference on Computer and Information Technology. – Bradford, West Yorkshire, UK, 2010. – Pp. 824-831.
6. Anisimov, V.F. Otvetstvennost' za prestupleniya protiv sobstvennosti s priznakami hishheniya: sostojanie, sushhnost' i problemy kvalifikacii: dis. ... d-ra jurid. nauk / V.F. Anisimov. – SPb., 2007. – 381 s.
7. Idrisov, N.T. O protivodejstvii recidivnoj prestupnosti (na osnove praktiki Sledstvennogo komiteta



Rossijskoj Federacii) / N.T. Idrisov // Juridicheskij vestnik Samarskogo universiteta. – 2018. – T. 4. № 2. – S. 61-64.

8. Kamyshanskij, V.P. Pravo sobstvennosti: predely i ogranichenija: monografija / V.P. Kamyshanskij. – M.: JuNITI, 2000. – 301 s.

9. Pletnev, D.A. Institucional'nye osnovy prav sobstvennosti / D.A. Pletnev // Vestnik Cheljabinskogo universiteta. Seriya 8: Jekonomika. Sociologija. Social'naja rabota. – 2006. – № 1. – S. 130-135.

10. Skljarov, S. Ugolovnaja otvetstvennost' za hishhenie nedvizhimogo imushhestva [Jelektronnyj resurs] / S. Skljarov // Rossijskaja justicija. – 2001. – № 6. – Rezhim dostupa: <https://base.garant.ru/987536/> (data obrashhenija: 03.01.2026).

11. Parfenov, M.R. K voprosu ob osobennostjah moshennichestva v sfere oborota nedvizhimosti s tochki zrenija neobходимости vnesenija izmenenij v dejstvujushhee zakonodatel'stvo / M.R. Parfenov // Evrazijskij Sojuz uchenyh. – 2014. – № 5-5 (5). – S. 155-159.

12. Pleshchikaja, H. Otvetstvennost' rieltora: za chto i kak otvechaet rieltor? / H. Pleshchikaja // Zhilishhnoe pravo. – 2014. – № 8. – S. 59-60.

АВТОРЛАР ТУРАЛЫ МӘЛІМЕТТЕР / СВЕДЕНИЯ ОБ АВТОРАХ / INFORMATION ABOUT AUTHORS

Талғат Смағұлұлы Салкебаев – Қазтұтынуодағы Қарағанды университетінің экономикалық қатынастарды құқықтық реттеу кафедрасының доценті, философия докторы (PhD), e-mail: salkebaev@mail.ru.

Салкебаев Талғат Смағұлович – доцент кафедры правового регулирования экономических отношений Карагандинского университета Казпотребсоюза, доктор философии (PhD), e-mail: salkebaev@mail.ru.

Salkebaev Talgat Smagulovich – Associate Professor Department of Legal Regulation of Economic Relations Karaganda University Kazpotrebsoyuz, PhD, e-mail: salkebaev@mail.ru.

Руслан Кайратович Джиембаев – Б. Бейсенов атындағы Қазақстан Республикасы Ішкі істер министрлігінің Қарағанды академиясының жалпы заң пәндері кафедрасының бастығы, заң ғылымдарының кандидаты, қауымдастырылған профессор, e-mail: rusya-our@mail.ru.

Джиембаев Руслан Кайратович – начальник кафедры общеюридических дисциплин Карагандинской академии Министерства внутренних дел Республики Казахстан имени Б. Бейсенова, кандидат юридических наук, ассоциированный профессор, e-mail: rusya-our@mail.ru.

Dzhiembaev Ruslan Kairatovich – Head of the Department of General Legal Disciplines of the Karaganda Academy of the Ministry of Internal Affairs of the Republic of Kazakhstan named after B. Beisenov, Candidate of Law, Associate Professor, e-mail: rusya-our@mail.ru.