



УДК 343.2/7
МРНТИ 10.77.01

Е.Е. Хамит

*Карагандинская академия Министерства внутренних дел Республики Казахстан
имени Б. Бейсенова, г. Караганда, Республика Казахстан*

ОСОБЕННОСТИ КВАЛИФИКАЦИИ ИНТЕРНЕТ-ХИЩЕНИЙ, СОВЕРШАЕМЫХ ПОСРЕДСТВОМ «ФИШИНГА»

Аннотация. Статья посвящена рассмотрению вопросов квалификации хищений, совершаемых посредством сети интернет и технических достижений путем использования персональных данных третьих лиц (реквизитов банковских счетов и карт, CVC-кодов и т.д.), полученных при совершении «фишинга». Раскрыта сущность понятия «фишинг» и рассмотрены условия, при которых данные, полученные рассматриваемым путем могут быть использованы как для совершения интернет-мошенничества, так и для совершения интернет-краж. Указывается, что весьма важным является то обстоятельство, что между фактом получения персональных данных и совершением хищения денежных средств может пройти определенный промежуток времени, который следует учитывать при квалификации деяния. Автором на основе анализа литературных источников по изучаемой проблематике и исследования опыта правоприменительной практики, предложены пути решения проблемных вопросов, связанных с квалификацией рассматриваемых деяний.

Ключевые слова: интернет-хищение; кибер-преступление; фишинг; персональные данные; квалификация деяния; обман; уголовная ответственность; банковские реквизиты; интернет-мошенничество; интернет-кража.

Е.Е. Хамит

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

«ФИШИНГ» АРҚЫЛЫ ЖАСАЛАТЫН ИНТЕРНЕТ-ЖЫМҚЫРУЛАРДЫ САРАЛАУДЫҢ ЕРЕКШЕЛІКТЕРІ

Аннотация. Мақала «фишинг» жасау кезінде алынған үшінші тұлғалардың дербес деректерін (банктік шоттар мен карталардың деректемелері, CVC-кодтар және т.б.) пайдалану арқылы интернет желісі және техникалық жетістіктер арқылы жасалатын жымқыруларды саралау мәселелерін қарауға арналған. «Фишинг» ұғымының мәні ашылады және қарастырылып отырған жолмен алынған деректерді интернет-алаяқтық жасау үшін де, интернет-ұрлық жасау үшін де пайдалануға болатын жағдайлар қарастырылады. Дербес деректерді алу фактісі мен ақша қаражатын жымқыру арасында белгілі бір уақыт өтуі мүмкін, оны іс-әрекетті саралау кезінде ескеру қажет. Автор зерттелетін мәселелер бойынша әдеби дереккөздерді талдау және құқық қолдану практикасының тәжірибесін зерттеу негізінде қарастырылып отырған іс-әрекеттерді саралауға байланысты проблемалық мәселелерді шешу жолдарын ұсынды.

Түйінді сөздер: интернет-жымқыру; кибер-қылмыс; фишинг; дербес деректер; іс-әрекетті саралау; алдау; қылмыстық жауапкершілік; банк деректемелері; интернет-алаяқтық; интернет-ұрлық.

Е.Е. Khamit

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

FEATURES OF QUALIFICATION OF INTERNET THEFT COMMITTED BY MEANS OF «PHISHING»

Abstract. The article is devoted to the issues of qualification of thefts committed via the Internet and technical



achievements through the use of personal data of third parties (bank account and card details, CVC codes, etc.) obtained during the commission of «phishing». The essence of the concept of «phishing» is revealed and the conditions under which the data obtained in this way can be used both to commit the Internet fraud and to commit Internet theft are considered. It is indicated that it is very important that a certain period of time may pass between the fact of obtaining personal data and the commission of embezzlement of funds, which should be taken into account when qualifying the act. The author, based on the analysis of literary sources on the studied issues and the study of the experience of law enforcement practice, suggests ways to solve problematic issues related to the qualification of the acts under consideration.

Keywords: Internet theft; cyber crime; phishing; personal data; qualification of the act; fraud; criminal liability; bank details; Internet fraud; Internet theft.

DOI: 10.52425/25187252_2023_29_67

Введение. Цифровые показатели, характеризующие современную преступность в Республике Казахстан (далее – РК), говорят о том, что на сегодняшний день, преступники в качестве средства совершения уголовно-наказуемых деяний активно осваивают и используют достижения технического прогресса и новых информационных технологий. В частности, такие виды хищений как кража и мошенничество стали регистрироваться

на много чаще за последние пять лет, потому как новым способом их совершения является использование возможностей информационных технологий. В данной научной статье мы подробнее исследуем проблемы квалификации данных деяний, поскольку не только данные правовой статистики (Таблица 1)¹, но и анализ правоприменительной практики указывают на такую необходимость.

	Статья УК РК	2017	2018	2019	2020	2021	2022
1	188 ч. 2 п. 4	112	240	518	750	1 591	1 954
2	190 ч. 2 п. 4	2 047	4 295	7 553	12 736	18 724	20 569

Таблица 1. Сведения о зарегистрированных фактах интернет-хищений по Республике Казахстан в период с 2017 по 2022 гг.

Как показывает анализ собранных данных социологического опроса, наличие многообразия среди способов совершения интернет-краж и интернет-мошенничеств, вызывает в практической деятельности у лиц, осуществляющих расследование некоторые сложности, связанные с их

квалификацией. Так, из 100% опрошенных респондентов – действующих сотрудников следственных подразделений РК, 68% испытывают сложности при установлении квалификации краж и мошенничеств, совершенных с использованием сети интернет (Рис. 1).

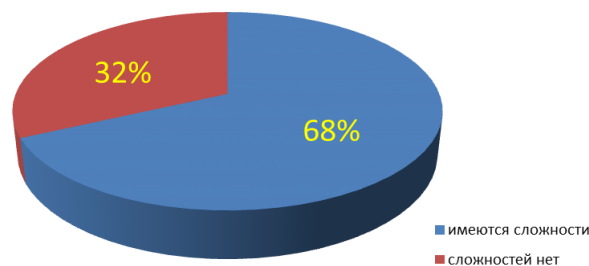


Рисунок 1. Процентное соотношение ответов респондентов на вопрос о наличии сложностей при установлении квалификации кибер-хищений

¹ Статистические данные – сведения об уголовных правонарушениях за 2017-2022 год / Портал органов правовой статистики и специальных учетов [Электронный ресурс] – Режим доступа: <https://qamqor.gov.kz/crimestat/statistics/> (дата обращения 12.05.2023).



Как показывает практика, на сегодняшний день большинство хищений в интернете совершаются при использовании персональных данных третьих лиц, полученных путем «фишинга».

Вышеуказанные обстоятельства актуализируют избранную тематику научной статьи, целью которой является освещение проблем, связанных с определением квалификации краж и мошенничеств, совершенных посредством сети интернет с использованием персональных данных третьих лиц. Как правило, иные виды хищений (присвоение или растрата вверенного чужого имущества, грабеж, разбой) весьма редко совершаются с использованием сети интернет и к слову, отдельного квалифицирующего состава в нормах Уголовного кодекса РК (далее – УК РК) не имеют. В этой связи, в данной работе рассматриваются проблемы квалификации кражи и мошенничества.

Материалы и методы. При подготовке данной научной статьи использовались эмпирические материалы, полученные в процессе диссертационного исследования, статистические данные, результаты анкетирования и интервьюирования респондентов.

Методологию данного научного исследования составляют общенаучные (сравнительный, системный, методы наблюдения, анализа и синтеза и др.), частнонаучные (статистический, социологический) и специальные (сравнительно-правовой, формально-юридический) правовые методы, с помощью которых сформулированы результаты исследования и предложены пути решения выявленных проблем.

Результаты и их обсуждение. Следует отметить, что наиболее важным элементом, влияющим на квалификацию рассматриваемых деяний, является объективная сторона и именно при совершении «фишинга», бывает весьма сложно различить какой вид хищения был совершен.

При традиционном мошенничестве объективная сторона уголовного правонарушения заключается в противоправном безвозмездном завладении чужим имуществом или правом на имущество путем обмана или злоупотребления доверием с целью обратить это имущество в свою пользу или пользу других лиц [1].

При совершении традиционной кражи объективная сторона состоит в тайном хищении чужого имущества.

Совершение вышеуказанных преступлений с использованием сети интернет представляет собой квалифицированный состав. Так, ответственность за совершение мошенничества, с использованием интернет сети предусмотрена пунктом 4 части 2 статьи 190 УК РК, а за совершение кражи – пунктом 4 части 2 статьи 188 УК РК².

Вместе с тем, в практической деятельности возникают вопросы квалификации не только краж и мошенничеств, совершаемых традиционными способами, но и совершаемых с использованием информационных технологий, о чем указывается в работах казахстанских исследователей³ [2]; [3]. Наибольшее внимание в данной научной статье мы бы хотели уделить такому явлению как «фишинг», поскольку именно его особенности влияют на квалификацию рассматриваемых деяний.

Во-первых, следует определиться, что же представляет собой «фишинг». Анализ множества научных работ исследователей уголовного права показывает, что «фишинг» представляет собой получение путем обмана или методом социальной инженерии (хакерства с использованием человеческого фактора) персональных данных для использования в корыстных, преступных целях [4]; [5].

Вместе с тем, становится не совсем ясно, почему же данный термин очень часто сопоставляют с интернет-мошенничеством [6]; [7]; [8], поскольку целью незаконного получения персональной информации не всегда является совершение хищений, это

² Уголовный кодекс Республики Казахстан: от 3 июля 2014 г. №226-V (с изм. и доп. по сост. на 20.05.2023 г.) [Электронный ресурс] – Режим доступа: https://online.zakon.kz/Document/?doc_id=31575252&pos=2874;-59#pos=2874;-59 (дата обращения: 20.07.2023).

³ Мошенничество: проблемы в законодательстве Республики Казахстан [Электронный ресурс] – Режим доступа: <https://articlekz.com/article/18695> (дата обращения: 20.07.2023).



может быть шантаж, угроза и т.д. Кроме того, по законодательству РК, мошенничество представляет собой применение обмана или злоупотребления доверием с целью получения имущества или права на имущество, а информацию о персональных данных нельзя признавать имуществом.

Согласно пункту 2 статьи 1 Закона РК «О персональных данных», персональные данные – сведения, относящиеся к определенному или определяемому на их основании субъекту персональных данных, зафиксированные на электронном, бумажном и (или) ином материальном носителе⁴.

С точки зрения гражданского права, имущество представляется в виде вещей (движимое и недвижимое имущество), денег (наличные и безналичные денежные средства), в том числе иностранной валюты, ценных бумаг, работ, услуг, объективированных результатов творческой интеллектуальной деятельности, фирменных наименований, товарных знаков и иных средств индивидуализации изделий (ст. 115 ГК РК)⁵.

Кроме того, информацию о своих персональных данных люди оставляют повсеместно: при регистрации на сайтах государственных услуг, в государственных учреждениях, в местах работы, на сайтах интернет-магазинов и т.д., что, несомненно, указывает на отсутствие качеств имущества у такой информации. Что касается банковских реквизитов – они хранятся не только в интернете, но и в самих отделениях банка, кредитных организациях и т.д.

Таким образом, представляется не вполне верным сопоставлять персональные данные с имуществом, в связи с чем, на наш взгляд, недопустимо отождествлять «фишинг» с мошенничеством.

Весьма интересным представляется и тот факт, что анализ УК РК показал, что сами по себе действия, охватываемые «фишингом», не предусмотрены ни в одной норме. Вместе с тем, «фишинг» является административным правонарушением, если данными действиями не был причинен

существенный вред правам и законным интересам лица.

Так, в УК РК имеется статья 147, которая регламентирует ответственность за нарушение неприкосновенности частной жизни и законодательства РК о персональных данных и их защите. В части второй данной статьи указано, что к уголовной ответственности привлекается лицо, незаконно осуществлявшее сбор и (или) обработку персональных данных в случаях, когда его действиями был причинен существенный вред правам и законным интересам лица.

То есть сам по себе сбор, и даже реализация (продажа) персональных данных не имеет в своем роде состава преступления, пока данными действиями не будет причинен существенный вред.

При этом, на наш взгляд, именно данное обстоятельство делает «фишинг» средством совершения уголовно-наказуемых хищений.

Само по себе слово «средство» означает определенный прием или способ действия, с помощью которого можно достичь желаемого, а также как орудие или предмет для осуществления деяния. Если рассматривать его с философской точки зрения, то охватить данный термин практически невозможно из-за его широты – под него подпадает все то, что субъект, который совершил преступление, мог использовать для того, чтобы достичь конечной цели [9].

Полученная персональная информация в рассматриваемых случаях подобна какому-либо предмету совершения преступления, применяемому для облегчения совершения преступного деяния или для более беспрепятственного достижения преступного результата. К примеру, как отвертка или лом, покупка которых законом не запрещена, но они могут быть использованы при взломе замка в квартире или двери автомобиля, облегчая тем самым доступ к имуществу.

Но здесь следует обратить внимание на саму сущность применения похищаемой информации. Так, если в случаях с отверткой, она не всегда может быть использована в

⁴ О персональных данных и их защите: закон Республики Казахстан от 21 мая 2013 г. №94-V // Казахстанская правда. – 2013. – 25 мая. – №178-179 (27452-27453).

⁵ Гражданский кодекс Республики Казахстан: от 27 дек. 1994 г. №268-XIII // Ведомости Верховного Совета Республики Казахстан, 1994 г. – №23-24.



преступных целях, то сложно представить себе факт получения незаконно собранной информации о персональных данных в благих, а равно – не в преступных целях.

На наш взгляд, является большим упущением законодателя то, что сам по себе факт незаконного сбора информации о персональных данных, который совершается зачастую с применением обмана и с использованием достижений технического прогресса, является уголовно-наказуемым лишь в случаях причинения существенного вреда.

На основании вышеизложенного, учитывая истинные цели «фишинга», мы справедливо приходим к выводу о том, что его следует понимать как незаконный сбор информации о персональных данных третьих лиц с использованием возможностей информационных систем и сети интернет, осуществляемый путем обмана или злоупотребления доверием.

Далее, мы подробнее рассмотрим случаи применения незаконно собранной информации о персональных данных третьих лиц в случаях совершения краж и мошенничеств с использованием сети интернет, для того, чтобы разобраться с особенностями квалификации данных деяний:

1. Если наряду с «фишингом» одновременно производятся действия по обману владельца персональных данных путем производства телефонного звонка, с целью получения его денежных средств незамедлительно, то в данных случаях, деяние следует квалифицировать как интернет-мошенничество.

Рассмотрим пример: Если при заполнении на «фишинговом» сайте персональных данных или совершении онлайн-покупки, указывается обязательное требование о связи с менеджером компании или преступники самостоятельно осуществляют звонок потерпевшему, требуя подтверждения анкетных данных, сообщая ложную информацию о задержке доставки, об отсутствии нужного товара и всячески пытаются ввести потерпевшего в заблуждение, то в данном случае, деяние

должно квалифицироваться по совокупности преступлений, а именно по части 2 статьи 147 УК РК и по пункту 4 части 2 статьи 190 УК РК (мошенничество). При этом, следует в обязательном порядке учитывать факт причинения значительного ущерба правам и законным интересом личности, однако справедливо отметить, что сам по себе факт совершения хищения имущества уже нарушает права и законные интересы лица. Данное обстоятельство связано с тем, что в рассматриваемом случае, наряду с незаконным получением персональных данных, осуществляется обман или введение в заблуждение с целью завладения имуществом потерпевшего и собственно, сам «фишинговый» сайт был создан с целью незаконного завладения чужого имущества (денежных средств).

2. Если полученные путем «фишинга» персональные данные были в последующем проданы третьему лицу, которое используя данную информацию, совершает такие действия как: списание денежных средств со счета или с банковской карты, оформление онлайн-покупок и т.д., то данные действия следует квалифицировать как интернет-кражу, но также как и в первом рассматриваемом случае, по совокупности с преступлением, предусмотренным частью 2 статьи 147 УК РК. Данная авторская позиция связана с тем, что третье лицо, получившее персональные данные для последующего совершения интернет-кражи, исходя из понятия «сбор», регламентированного в Законе РК «О персональных данных», уже совершает преступление, охватываемое объективной стороной деяния, указанного в части 2 статьи 147 УК РК. Кроме того, оно совершает хищение (списание денежных средств со счета или онлайн-покупки) в тайне от владельца имущества, не применяя никакого обмана.

Напомним, что в соответствии с положениями нормативного постановления Верховного Суда РК от 29 июня 2017 года №6 «О судебной практике по делам о мошенничестве», при совершении мошенничества обман производится с целью хищения имущества или приобретения



права на чужое имущество и направлен непосредственно на владельца имущества или иное лицо, которому вверено данное имущество (ч. 2)⁶. В случае же, с совершением хищения денежных средств путем использования ранее незаконно собранных персональных данных, такой обман отсутствует.

При этом, также хотелось бы отметить, что вышеуказанные примеры совершения «фишинга» не будут требовать дополнительной квалификации по статье 205 УК РК (неправомерный доступ к информации, в информационную систему или сеть телекоммуникаций), поскольку такой квалифицирующий признак как «использование информационной системы» уже присутствует в частях четвертых статей 190 и 188 УК РК.

Таким образом, «фишинг» представляет собой лишь незаконное получение персональных данных (ложные сайты, письма с требованием подтвердить личные данные, использование различных специальных технических средств и т.д.) с целью дальнейшего совершения преступления, посредством их использования. Тем не менее, весьма важным является то обстоятельство, что между фактом получения персональных данных и совершением хищения денежных средств может пройти определенный промежуток времени, который следует учитывать при квалификации деяния. Кроме того, преступник может использовать персональные данные самостоятельно или же продать их в «даркнете», что тоже является не маловажным фактом для правильной квалификации содеянного. Приведем еще один пример: «Работая официантом в одном из увеселительных заведений города Нур-Султан, Т. при оплате счета посетителями с помощью POS-терминала, используя свое служебное положение, злоупотреблял доверием клиентов и списывал реквизиты их банковских карт, т.е. занимался «фишингом». В дальнейшем, используя ранее полученные реквизиты, Т.

через Интернет-банкинг совершал хищения денег с банковских карт. Действия гр. Т. были квалифицированы по пункту 4 части 2 статьи 188 УК РК» [10]. Рассматривая данный факт, справедливо хотелось бы отметить, что в данном случае, содеянное следовало бы квалифицировать по совокупности преступлений, а именно, наряду со статьей 188 УК РК, следует привлекать к ответственности по части 2 статьи 147 УК РК.

Для правильной квалификации рассматриваемых деяний важно также учитывать, на что был изначально направлен умысел лица, совершившего «фишинг», т.е. на что конкретно были направлены действия по незаконному получению персональной информации о банковских счетах, картах и т.д. и совершались ли они одновременно с обманом владельца имущества для непосредственного совершения хищения или же хищение осуществлялось в тайне.

Заклучение. Так, подробное рассмотрение сущности такого понятия как «фишинг» и случаев применения персональной информации, полученной данным способом при совершении интернет-хищений, справедливо позволило прийти к следующим выводам:

- учитывая истинные цели «фишинга», его следует понимать как незаконный сбор информации о персональных данных третьих лиц с использованием возможностей информационных систем и сети интернет, осуществляемый путем обмана или злоупотребления доверием;

- если персональные данные, собранные путем «фишинга» были куплены в интернете или получены любым другим способом от третьих лиц, а в последующем с их помощью произошло хищение денежных средств с банковского счета или с карты, то данное деяние следует квалифицировать по совокупности преступлений: по пункту 4 части 2 статьи 188 УК РК (кража) и по части 2 статьи 147 УК РК. Таким образом, лицо, похищая денежные средства с карты или с банковского счета, именно в момент совершения своих преступных действий не

⁶ О судебной практике по делам о мошенничестве: нормативное постановление Верховного Суда РК от 29 июня 2017 г. №6 // Казахстанская правда. – 2017. – 27 июля. – №142 (28521).



использует никакого обмана, поскольку все необходимые персональные данные уже у него имеются, но одновременно причиняет существенный вред законным правам и интересам личности (конституционное право на неприкосновенность имущества). Также, данные действия происходят тайно, что непосредственно представляет собой признак кражи, а не мошенничества;

- если же незаконный сбор персональных данных изначально был направлен на совершение хищений и такой сбор сопровождался непосредственным контактом с владельцем персональных данных, который был введен в заблуждение или обманут с целью завладения его имуществом, – здесь справедливо квалифицировать содеянное по пункту 4 части 2 статьи 190 УК РК (мошенничество), но также по совокупности с частью 2 статьи 147 УК РК.

При этом, не требуется дополнительной квалификации по статье 205 УК РК (неправомерный доступ к информации, в информационную систему или сеть телекоммуникаций), поскольку такой квалифицирующий признак как «использование информационной системы» уже присутствует в частях четвертых, в статьях 190 и 188 УК РК.

В первом случае (при совершении кражи), на наш взгляд, несомненно, присутствуют два оконченных факта незаконных действий – сбор персональной информации и хищение денежных средств. При этом первое действие может совершаться совершенно другим субъектом, который не будет причастен к совершению кражи. Однако, в УК РК нет подходящего состава преступления, которым возможно было бы квалифицировать действия по хищению личной информации,

без причинения существенного вреда, что на наш взгляд пагубно отражается на профилактике совершения любых уголовно-наказуемых деяний, совершение которых возможно посредством использования персональных данных и, несомненно, представляет собой пробел в казахстанском законодательстве.

В этой связи, в целях исключения проблем, связанных с квалификацией интернет-хищений, совершаемых посредством использования информации о персональных данных полученной путем «фишинга» и дальнейшего совершенствования уголовного законодательства в целях предупреждения фактов кибер-преступлений, необходимо:

1. Во всех случаях совершения «фишинга» устанавливать цель и умысел совершения данного деяния.

2. В случаях, когда «фишинг» совершен как отдельное самостоятельное деяние – целесообразно рассматривать его как самостоятельный состав правонарушения, даже в случаях отсутствия причинения существенного вреда правам и законным интересам личности. В этой связи, на наш взгляд, в целях предупреждения совершения любых уголовно-наказуемых деяний с использованием незаконно полученных персональных данных, справедливо перевести из кодекса РК об административных правонарушениях деяние, предусмотренное в статье 79 «Нарушение законодательства Республики Казахстан о персональных данных и их защите» и ввести его в УК РК. Наиболее подходящим, на наш взгляд, видится внесение изменений в статью 147 УК РК.

Список использованной литературы:

1. Togaibayeva, S.S. Features of the commission of fraud, coupled with the failure to comply with the provisions of a civil contract / S.S. Togaibayeva, et al. // Journal of Politics and Law. – 2019. – №3(12). – С. 69-79.
2. Жолжаксынов, Ж.Б. Хищение посредством использования информационно-коммуникационных технологий в уголовном законодательстве Республики Казахстан / Ж.Б. Жолжаксынов, Е.Б. Жунусов // «Хабаршы – Вестник» Карагандинской академии МВД Республики Казахстан им. Б. Бейсенова. – 2021. – №2(72). – С. 20-25.
3. Калиев, А.А. Киберпреступность – новая глобальная угроза / А.А. Калиев // Құқық қорғау



органдары академиясының Жаршысы. – 2018. – №2(8). – С. 14-20.

4. Lastdrager, E.E. Achieving a consensual definition of phishing based on a systematic review of the literature [Electronic resource] / E.E. Lastdrager // Crime Science Journal. – 2014. – №3. – Access mode: <https://crimesciencejournal.biomedcentral.com/articles/10.1186/s40163-014-0009-y> (Access data: 20.05.2023).

5. Purkait, S. Phishing counter measures and their effectiveness – literature review / S. Purkait // Information Management & Computer Security. – 2012. – №20(5). – Pp. 382-420.

6. Moore, T. Phishing and the economics of e-crime / T. Moore // Infosecurity. – 2007. – №4(6). – Pp. 34-37.

7. Hong, J. The state of phishing attacks / J. Hong // Communications of the ACM. – 2012. – №55(1). – Pp. 74-81.

8. Батюшкин, М.В. «Фишинг» – компьютерное мошенничество? [Электронный ресурс] / М.В. Батюшкин // Символ науки. – 2021. – №1. – Режим доступа: <https://cyberleninka.ru/article/n/fishing-kompyuternoe-moshennichestvo> (дата обращения: 15.05.2023).

9. Поляков, В.В. Средства совершения компьютерных преступлений [Электронный ресурс] / В.В. Поляков, С.А. Лапин // Доклады ТУСУР. – 2014. – №2(32). – Режим доступа: <https://cyberleninka.ru/article/n/sredstva-soversheniya-kompyuternyh-prestupleniy> (дата обращения: 16.05.2023).

10. Еспергенова, Е.В. Некоторые вопросы квалификации преступлений, связанных с хищением денежных средств со счетов банковских карт / Е.В. Еспергенова // «Хабаршы – Вестник» Карагандинской академии МВД Республики Казахстан им. Б. Бейсенова. – 2021. – №2(72). – С. 14-19.

References:

1. Togaibayeva, S.S. Features of the commission of fraud, coupled with the failure to comply with the provisions of a civil contract / S.S. Togaibayeva, et al. // Journal of Politics and Law. – 2019. – №3(12). – S. 69-79.

2. Zholzhaksynov, Zh.B. Hishhenie posredstvom ispol'zovaniya informacionno-kommunikacionnyh tehnologij v ugovnom zakonodatel'stve Respubliki Kazahstan / Zh.B. Zholzhaksynov, E.B. Zhunusov // «Habarshy – Vestnik» Karagandinskoj akademii MVD Respubliki Kazahstan im. B. Bejsenova. – 2021. – №2(72). – S. 20-25.

3. Kaliev, A.A. Kiberprestupnost' – novaja global'naja ugroza / A.A. Kaliev // Құқық қорғау органдары академиясының Жаршысы. – 2018. – №2(8). – С. 14-20.

4. Lastdrager, E.E. Achieving a consensual definition of phishing based on a systematic review of the literature [Electronic resource] / E.E. Lastdrager // Crime Science Journal. – 2014. – №3. – Access mode: <https://crimesciencejournal.biomedcentral.com/articles/10.1186/s40163-014-0009-y> (Access data: 20.05.2023).

5. Purkait, S. Phishing counter measures and their effectiveness – literature review / S. Purkait // Information Management & Computer Security. – 2012. – №20(5). – Pp. 382-420.

6. Moore, T. Phishing and the economics of e-crime / T. Moore // Infosecurity. – 2007. – №4(6). – Pp. 34-37.

7. Hong, J. The state of phishing attacks / J. Hong // Communications of the ACM. – 2012. – №55(1). – Pp. 74-81.

8. Batjushkin, M.V. «Fishing» – komp'yuternoe moshennichestvo? [Elektronnyj resurs] / M.V. Batjushkin // Simvol nauki. – 2021. – №1. – Rezhim dostupa: <https://cyberleninka.ru/article/n/fishing-kompyuternoe-moshennichestvo> (data obrashheniya: 15.05.2023).

9. Poljakov, V.V. Sredstva soversheniya komp'yuternyh prestuplenij [Elektronnyj resurs] / V.V. Poljakov, S.A. Lapin // Doklady TUSUR. – 2014. – №2(32). – Rezhim dostupa: <https://cyberleninka.ru/article/n/sredstva-soversheniya-kompyuternyh-prestupleniy> (data obrashheniya: 16.05.2023).

10. Espergenova, E.V. Nekotorye voprosy kvalifikacii prestuplenij, svjazannyh s hishheniem denezhnyh sredstv so schetov bankovskih kart / E.V. Espergenova // «Habarshy – Vestnik»



АВТОРЛАР ТУРАЛЫ МӘЛІМЕТТЕР / СВЕДЕНИЯ ОБ АВТОРАХ / INFORMATION ABOUT AUTHORS

Еділ Едігеұлы Хамит – Қазақстан Республикасы Ішкі істер министрлігінің Б. Бейсенов атындағы Қарағанды академиясының докторанты, заң ғылымдарының магистрі, e-mail: n_zan_kz@mail.ru.

Хамит Еділ Едігеұлы – докторант Карагандинской академии Министерства внутренних дел Республики Казахстан имени Б. Бейсенова, магистр юридических наук, e-mail: n_zan_kz@mail.ru.

Khamit Edil Edigeuly – doctoral student of the Karaganda Academy of the Ministry of Internal Affairs of the Republic of Kazakhstan named after B. Beisenov, Master of Law, e-mail: n_zan_kz@mail.ru.