УДК 343.985.7
ГРНТИ 10.85.51

ОТДЕЛЬНЫЕ АСПЕКТЫ РАССЛЕДОВАНИЯ ИНТЕРНЕТ-МОШЕННИЧЕСТВА

Калиев Аскар Абужанович
Магистр права, доцент кафедры специальной подготовки по противодействию глобальным угрозам Института профессионального обучения Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан; г. Косшы, Республика Казахстан; e-mail: askar909@mail.ru; ORCID: https://orcid.org/0009-0006-3621-7107

Аннотация. *Современные технологии и цифровизация являются ключевыми причинами распространения киберпреступности в мире. В зависимости от степени их применения различают две категории преступлений: первая - киберзависимые преступления и вторая - преступления, совершаемые с использованием кибертехнологий.*

В данной статье рассматривается одно из наиболее распространенных киберпреступлений, относящихся ко второй категории – интернет-мошенничество. Автором проанализированы отдельные аспекты данного вида преступления, понятие и его основные виды, причины распространения и слабой раскрываемости дел правоохранительными органами. Затронуты вопросы необходимости постоянного совершенствования методики борьбы с интернет-мошенничеством, путём повышения квалификации сотрудников правоохранительных органов, внедрения новых образовательных программ или отдельных учебных модулей и использования современных технологий таких как блокчейн или искусственный интеллект. Акцентировано внимание на использовании преступниками криптовалют с целью сокрытия следов преступной деятельности. Раскрыты особенности некоторых видов цифровых активов популярных среди лиц, совершающих уголовные правонарушения.

Основное внимание в работе уделено современным методам расследования таких преступлений, с акцентом на важность электронных доказательств и анализ цифровых следов. Автор статьи подчеркивает необходимость создания целевой системы борьбы с интернет-мошенниками, путем внедрения организационных и технических методов противодействия, а также усиления превентивных мер способных минимизировать количество преступлений данного вида.

Результаты данного исследования могут быть использованы при составлении специализированных образовательных программ для сотрудников правоохранительных органов, задействованных в расследовании киберпреступлений, а также для разработки более эффективных методов выявления и пресечения интернет-мошенничества.

Ключевые слова: *Интернет, киберугроза, мошенничество, искусственный интеллект, криптовалюта, блокчейн, новые технологии, киберпреступность.*

ИНТЕРНЕТТЕГІ АЛАЯҚТЫҚТЫ ТЕРГЕУДІҢ ЖЕКЕЛЕГЕН АСПЕКТІЛЕРІ

Асқар Әбужанұлы Қалиев
Құқық магистрі, Қазақстан Республикасының Бас прокуратурасы жанындағы Құқық қорғау органдары академиясының Кәсіби оқыту институтының Жаһандық қауіп-қатерлерге қарсы іс-қимыл жөніндегі арнайы дайындық кафедрасының доценті; Қосшы қ., Қазақстан Республикасы; e-mail: askar909@mail.ru; ORCID: https://orcid.org/0009-0006-3621-7107

Аннотация. *Заманауи технологиялар мен цифрландыру әлемде киберқылмыстың таралуының негізгі себептері болып табылады. Оларды қолдану деңгейіне байланысты қылмыстар екі санатқа бөлінеді: бірінші - киберге тәуелді қылмыстар және екінші - кибертехнологияларды пайдалану арқылы жасалатын қылмыстар.*

Бұл мақалада екінші санатқа жататын ең кең таралған киберқылмыстардың бірі – интернет-алаяқтық қарастырылады. Автор бұл қылмыс түрінің жекелеген аспектілерін, оның ұғымы мен негізгі түрлерін, таралу себептері мен құқық қорғау органдарының істерді нашар ашуының себептерін талдаған. Интернет-алаяқтықпен күресу әдістерін үнемі жетілдірудің маңыздылығы туралы мәселелер қозғалды, атап айтқанда, құқық қорғау органдары қызметкерлерінің біліктілігін арттыру, жаңа білім беру бағдарламаларын немесе жеке оқу модульдерін енгізу және блокчейн немесе жасанды интеллект сияқты заманауи технологияларды пайдалану. Қылмыскерлердің қылмыстық қызметінің іздерін жасыру мақсатында криптовалюталарды пайдалануына ерекше назар аударылды. Қылмыстық құқық бұзушылықтарды жасайтын тұлғалар арасында танымал кейбір цифрлық активтердің ерекшеліктері ашып көрсетілді.

Жұмыста осындай қылмыстарды тергеудің заманауи әдістеріне, әсіресе электрондық дәлелдемелердің маңыздылығы мен цифрлық іздерді талдауға ерекше көңіл бөлінген. Мақала авторы интернет-алаяқтармен күреске бағытталған жүйені құрудың қажеттілігін атап өтеді. Бұл жүйеге ұйымдастырушылық және техникалық қарсы іс-қимыл әдістерін енгізу, сондай-ақ осы санаттағы қылмыстар санын азайта алатын алдын алу шараларын күшейту жатады.

Осы зерттеу нәтижелері киберқылмыстарды тергеуге қатысатын құқық қорғау органдарының қызметкерлеріне арналған мамандандырылған білім беру бағдарламаларын әзірлеуде, сондай-ақ интернет-алаяқтықты анықтау және оны тоқтатудың неғұрлым тиімді әдістерін әзірлеуде пайдаланылуы мүмкін.

Түйінді сөздер: *Интернет, киберқауіп, алаяқтық, жасанды интеллект, криптовалюта, блокчейн, жаңа технологиялар, киберқылмыс.*

SELECTED ASPECTS OF THE INVESTIGATION OF INTERNET FRAUD

Askar Abuzhanovich Kaliyev
Master of Law, Associate Professor of the Department of Specialized Training on Countering Global Threats, Institute of Professional Training of the Academy of Law Enforcement Agencies under the General Prosecutor's Office of the Republic of Kazakhstan; Kosshy c., Republic of Kazakhstan; e-mail: askar909@mail.ru; ORCID: https://orcid.org/0009-0006-3621-7107

Abstract. *Modern technology and digitalization are key reasons for the spread of cybercrime in the world. Depending on the degree of their application, two categories of crime are distinguished: the first is cyber-related crime and the second is cyber-related crime.*

This article examines one of the most common cybercrimes belonging to the second category - Internet fraud. The author analyzes certain aspects of this type of crime, the concept and its main types, the reasons for the spread and poor solving of cases by law enforcement agencies. The questions of necessity of constant improvement of methods of struggle against Internet fraud, by means of improvement of qualification of employees of law enforcement bodies, introduction of new educational programs or separate training modules and use of modern technologies such as blockchain or artificial intelligence are touched upon. Emphasized the use of cryptocurrencies by criminals to hide traces of criminal activity.

The features of some types of digital assets popular among perpetrators of criminal offenses are disclosed.

The paper focuses on modern methods of investigation of such crimes, with emphasis on the importance of electronic evidence and analysis of digital traces. The author of the article emphasizes the need to create a targeted system of combating Internet fraudsters, through the introduction of organizational and technical methods of counteraction, as well as strengthening preventive measures that can minimize the number of crimes of this type.

The results of this study can be used in the development of specialized educational programs for law enforcement officers involved in the investigation of cybercrime, as well as for the development of more effective methods of detection and suppression of Internet fraud.

Keywords: *Internet, cyber threat, fraud, artificial intelligence, cryptocurrencie, blockchain, new technologies, cybercrime.*

DOI: 10.52026/2788-5291_2025_80_2_294

Введение

Повсеместное распространение интернета, развитие современных технологий и сама цифровизация гражданского общества способствовали появлению нового вида преступной деятельности, такого как интернет-мошенничество, которое повлияло на экономическую и социальную сферу жизнедеятельности людей.

Задачи и цели. Целью статьи является анализ различных видов интернет-мошенничества, методик, используемых лицами, совершающими мошенничество посредством интернета и других информационно-коммуникационных технологий. К задачам статьи относится исследование технических аспектов, включающих в себя технологии криптовалют, специализированные программные обеспечения, анонимность психологических аспектов, таких как социальная инженерия, правовых аспектов, предусматривающих рассмотрение механизмов противодействия интернет-мошенничества, в т.ч. на международном уровне и разработка предложений и рекомендаций по борьбе с ними с использованием правовых и технических условий.

Материалы и методы

Объектом исследования предстали научные работы в сфере киберпреступлений, нормативные акты, статистические данные и материалы уголовных правонарушений, связанных с интернет-мошенничеством.

В ходе исследования использован комплекс общенаучных методов и специальные методы юридической науки (формально-догматический, метод толкования).

Обсуждение и результаты

Киберпреступность на сегодняшний день представляет собой серьезную угрозу, как для общества, так и государства в целом, создавая препятствия для нормального функционирования современных цифровых систем. В этой связи уже давно назрела необходимость усиления роли профилактики в предотвращении и борьбы с данным видом преступлений и, в частности, с интернет-мошеничеством. Одним из важных ключевых аспектов должна стать информированность пользователей информационных систем о всевозможных угрозах и рисках, соблюдения ими кибергигиены, предусматривающей использование антивирусных программ, межсетевого экрана и других средств защиты от кибератак.

Согласно сведениям Комитета по правовой статистике и специальным учетам Генеральной прокуратуры Республики Казахстан, за период 2022-2024 гг. правоохранительными органами зарегистрировано 261 (2022 г.– 85, 2023 г. – 78, 2024 г. – 98) уголовное правонарушение. Из них в суд направлено 54 уголовных дела (2022 г. – 8, 2023 г. – 21, 2024 г. – 25). Прерваны сроки досудебного расследования по 60 уголовным правонарушениям (2022 г. – 12, 2023 г. – 13, 2024 г. – 35). При этом количество нераскрытых уголовных проступков, прекращенных за истечением сроков давности без лица составило 104 (2022 г. – 46, 2023 г. – 37, 2024 г. – 21)[1].

Все зарегистрированные уголовные правонарушения совершены с использованием сети Интернет, незаконным доступом в информационную систему и путем обмана или злоупотребления доверием пользователя информационной системы, к числу которых относится и интернет-мошенничество. Такая низкая раскрываемость преступлений в сфере информационно-коммуникационных технологий связана в первую очередь с дефицитом кадровых IT-специалистов в правоохранительных органах и судебных экспертов, высокой квалификации преступников и недостаточным количеством алгоритмов и методик расследования данных видов преступлений.

По данным Центра по борьбе с киберпреступностью Департамента криминальной полиции Министерства внутренних дел РК, в Казахстане интернет-мошенничество, также, как и во многих государствах мира, стало самым распространенным видом киберпреступлений, совершаемых с использованием кибертехнологий.

Представленные на нижеуказанном рисунке № 1 данные наглядно демонстрируют количество анализируемых интернет-преступлений на фоне общего количества всех зарегистрированных мошенничеств в стране.

[1] *Статистические отчеты № 1-М «О зарегистрированных уголовных правонарушениях» за 2022-2024 гг. // Портал органов правовой статистики и специальных учетов // URL: https://qamqor.gov.kz/crimestat/statistics (дата обращения: 02.09.2024).*

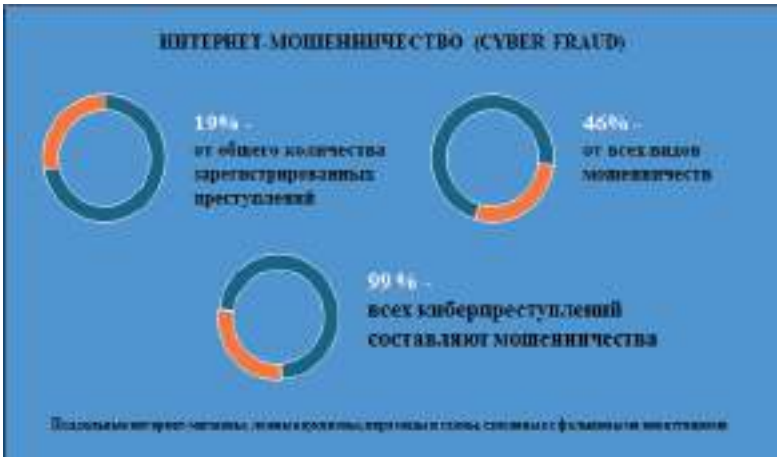

Рис. 1. Данные о количестве интернет – мошенничеств

Что представляет из себя интернет-мошенничество? Имеется различное понимание данного термина, интерпретация которого зависит от научного направления и подходов к исследованию данного явления.

Например, ряд таких ученых как Михаил Леви (Michael Levi)[2], Томас Холт (Thomas Holt)[3], считают, что нельзя относить интернет-мошенничество только к преступлению, совершаемому в рамках одного государства и лишь с применением интернет-инфраструктуры. Другие ученые, а именно Ян ван Дейк (Jan van Dijk) полагают, что к интернет-мошенничеству следует также отнести и злоупотребление конфиденциальной информацией, а не только материальные ценности, что представляют собой деньги [1]. Но, несмотря на различные подходы к формулировке и самое главное к пониманию данного феномена преступления, все они едины во мнении о многоаспектности явления интернет-мошенничества, сочетающего в себе традиционные формы преступности с новыми технологиями и психологическими приемами, раскрывающими смысл социальной инженерии.

Из всего вышеотмеченного следует, что интернет-мошенничество – это такая форма преступности, совершаемая в киберпространстве, при которой злоумышленники используют самые передовые средства и технологии коммуникаций для достижения своих целей (обмана, кражи денег и т.д.).

К ним можно отнести элементы социальной инженерии, при которой потерпевшие подвергаются такой психологической обработке, что заставляет их выполнить все указания злоумышленников, а также использование вредоносных компьютерных программ, в т.ч. по сокрытию цифровых следов в компьютерной системе и(или) в сети.

Поэтому для его понимания и расследования правоохранительными органами должен применяться комплексный, междисциплинарный подход, предполагающий изучение таких научных направлений как информационная безопасность, юридическая психология, криминология и криминалистика.

Кроме того, киберпреступления требуют от правоохранительных органов не только базовых знаний в области юриспруденции, но и глубокого понимания современных технологий, криптографии, принципов работы компьютерных сетей и систем безопасности [2, с. 11].

Похожую точку зрения высказывает и российский исследователь Р.С. Атаманов, предлагающий разработать и внедрить универсальную методику расследования, практическое применение которой будет способствовать увеличению количества выявляемых преступлений, относящихся к интернет-мошенничеству, и качеству их расследования [3].

Важным компонентом любой методики расследования является информация о методах и способах совершения преступления (интернет-мошенничества) и его отдельных видов.

Анализ материалов уголовных правонарушений, связанных с интернет-мошенничеством, позволил выделить следующие его виды:

1) Фишинг – вид интернет-мошенничества, цель которого заполучить конфиден-

[2] *States, frauds, and the threat of transnational organized crime, интернет-источник // URL: https://www.jstor.org/stable/24388250 (date of reference: 02.09.2024).*

[3] *Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offenses // URL: https://www.taylorfrancis.com/books/mono/10.4324/9781315775944/cybercrime-progress-thomas-holt-adam-bossler (date of reference: 02.09.2024).*

циальные данные пользователей (пароли, логины, номера кредитных карт, банковских счетов и другая важная информация)[4]. Чаще всего объектами их посягательств становятся логины и пароли граждан от ресурсов, содержащих банковскую информацию, а также другие персональные данные;

2) Инвестиционные схемы – вид интернет-мошенничества, при котором злоумышленники обещают гражданам высокую прибыль от инвестиций, предлагая вложить средства в вымышленные инвестиционные проекты или криптовалютные платформы[5];

3) Мошенничество в онлайн-торговле – вид интернет-мошенничества, при котором потерпевшие теряют свои деньги после посещения поддельных интернет-магазинов и получения оплаты злоумышленниками[6].

Для реализации своих преступных намерений злоумышленники используют различные средства коммуникации (мессенджеры, социальные сети, сайты, индексацию поисковых систем и т.д.). Поэтому, чтобы не стать жертвой интернет-преступников гражданам нужно очень осторожно относиться к различным непроверенным интернет-магазинам, проверять не только отзывы людей о торговой площадке, но и обращать внимание на их контактные данные, условия возврата товара и т.д.;

4) Мошенничество с использованием вредоносного программного обеспечения – вид интернет-мошенничества, при котором злоумышленники для хищения денег потерпевших используют различные вредоносные компьютерные программы[7].

На сегодняшний день одна из самых известных вредоносных программ, которые используют злоумышленники, называется «ransomware» – это программа-вымогатель, которая шифрует файлы на устройстве потерпевшего.

Целью преступников становятся не только простые граждане, но и государственные органы. Суть данного вида преступления заключается в следующем. Злоумышленники распространяют зараженные файлы или ссылки к ним через мессенджеры, поддельные сайты, электронную почту потерпевшим. Как только кто-нибудь по ним пройдет или откроет зараженную ссылку, они получают доступ к устройству потерпевшего и могут зашифровать данные, украсть информацию или деньги.

Большинство интернет-мошенничеств совершаются при помощи метода психологической манипуляции, когда потерпевший до конца не осознает противоправный характер намерений преступников. Иными словами, он основан на доверии граждан к действиям и словам злоумышленников. Во многих источниках и литературе такой метод совершения преступлений называется социальная инженерия, при которой используются эмоции людей (например, страх, доверие или просто элементарная человеческая жадность).

Сложность и опасность данного метода заключается в том, что такие преступления предотвратить очень сложно, как с правовой, так и технической точки зрения. Так как не существуют специальные программные обеспечения, которые смогли бы защитить пользователя информационной системы от мошенников.

Более того, вопрос успешного расследования и раскрытия интернет-мошенничеств усугубляется еще и рядом других причин, к числу которых следует отнести технические аспекты преступления. Это применение технологий защиты конфиденциальности: виртуальные частные сети (VPN), прокси – сервера, анонимайзеры – браузер Tor, SSH-туннели, которые маскируют данные пользователя, что обеспечивает анонимность преступников, безнаказанность их и способствует повышению интереса к ним.

Иногда из-за применения таких технологий раскрытие преступлений становится очень сложным, т.к. они позволяют преступникам маскировать свой реальный IP-адрес, использующийся для идентификации пользователя в сети интернет.

Другим аспектом, препятствующим раскрытию и расследованию преступлений

[4] *Что такое «фишинг» // Encyclopedia // URL: https://encyclopedia.kaspersky.ru/knowledge/what-is-phishing/#:~:text=%D0%A4%D0%B8%D1% 88%D0%B8%D0%BD%D0%B3%20(%D0%B0%D0%BD%D0%B3%D0%BB.%20phishing,%20%D0%BE%D1%82%20fishing%20 (дата обращения: 01.10.2024).*

[5] *Финансовый обман: как не попасться на уловки мошенников в сфере инвестиций // Международное информационное агентство «Казинформ» // URL: https://www.inform.kz/ru/finansoviy-obman-kak-ne-popastsya-na-ulovki-moshennikov-v-sfere-investitsiy-858a2e (дата обращения: 06.09.2024).*

[6] *Виды мошенничества // WesternUnion // URL: https://www.westernunion.com/kz/ru/fraudawareness/fraud-types.html (date of reference: 07.06.2024).*

[7] *О мошенничестве с использованием сети Интернет и сотовой связи // Администрация банковского муниципального района интернет-источник // URL: https://www.admbal.ru/news_all/o-moshennichestve-s-ispolzovaniem-seti-internet-i-sotovoy-svyazi/ (дата обращения: 07.06.2024).*

данной категории, является технология блокчейн и связанная с ней среда математических вычислений, к которой относятся криптовалюты.

Из-за своей анонимности и сложности отслеживания преступники давно заменили фиатные и электронные деньги на криптовалюты, которые помогают им оставаться безнаказанными. Наиболее распространенными и популярными видами криптовалют являются биткоин, эфириум, лайткин, монеро и др.

Среди основных особенностей, характеризующих криптовалюты является их децентрализация, т.е. отсутствие управляющего органа, который мог бы участвовать в их создании и управлении в качестве посредника, что делает их особенно привлекательными для преступников.

Несмотря на общие характеристики и способности каждой из перечисленных криптовалют, преступники отдают предпочтение самым технологичным, а именно трудно отслеживаемым. К числу данных криптовалют следует отнести такую монету как монеро (monero). Она больше всего используется злоумышленниками из-за ее особой анонимности.

В любом случае каждая из этих криптовалют имеет свою уникальность, т.к. все они используют технологию скрытых адресов и кольцевых подписей, что делает их идеальными для незаконных операций. В свою очередь это вызывает у следственных органов трудности в отслеживании и особенно в идентификации, когда необходимо определить источник или получателя эквивалента денежных средств.

Поэтому они применяются интернет-мошенниками, когда нужно скрыть следы своих действий, остаться анонимными и безнаказанными.

Еще одним из наиболее известных и популярных инструментов для сокрытия цифровых следов является браузер Tor (Top), предоставляющий пользователям услуги по маскировке их местоположения и сокрытию деятельности в интернете. Суть работы данного браузера заключается в перенаправлении всего объема интернет-трафика пользователя через несколько узлов, раскиданных по всему миру. То есть, использующий браузер Top пользователь интернета маскирует свой реальный IP-адрес, делая процесс идентификации практически невозможным.

Использование данной технологии также вызывает трудности у правоохранительных органов при организации и проведении расследования преступлений, связанных с интернет-мошенничеством.

Таким образом, следует отметить, что вопрос расследования интернет-мошенничества является не просто сложной, но и многогранной проблемой, требующей совместного участия правоохранительных органов и специалистов в области информационной безопасности. Это в свою очередь свидетельствует о необходимости постоянного повышения квалификации следователей, задействованных в расследовании интернет-мошенничеств. Они должны обладать знаниями в области электронных доказательств, поиска цифровых следов из-за использования преступниками средств анонимизации.

Помимо данных навыков следователи должны также развивать у себя навыки коммуникации с потерпевшими из-за когнитивных особенностей, совершенных в отношении них интернет-мошенничеств.

Тем самым, расследование интернет-мошенничеств требует использование психологических методов работы при организации и проведении расследования.

Кроме того, учитывая трансграничный характер киберпреступлений, в т.ч. и интернет-мошенничеств, следует уделять должное внимание и международному сотрудничеству в части организации работы с цифровыми доказательствами, их запросу из других стран.

В этом плане особое значение будет играть правовое обеспечение работы следственно-оперативных подразделений. Именно законодательное регулирование интернет-мошенничества является залогом успеха их расследования и привлечения виновных лиц к ответственности.

Одним из важных международных документов, рассматривающих вопросы борьбы с интернет-мошенничеством, и в целом с киберпреступностью является Будапештская конвенция о киберпреступности, принятая еще в 2001 году[8].

Данная международная Конвенция, признанная большинством стран, была разработана по инициативе Совета Европы и регламентирует основные вопросы борьбы с киберпреступлениями, в части международного сотрудничества в расследовании и преследовании преступников.

[8] *Будапештская конвенция // URL: https://www.coe.int/ru/web/impact-convention-human-rights/convention-on-cybercrime#/ (date of reference: 10.08.2024).*

В частности, Конвенция устанавливает обязанности для каждой из подписавшей ее страны по урегулированию законодательной базы и приведение ее в соответствие с международными стандартами.

Казахстан не является участником Будапештской конвенции, однако выражает заинтересованность в присоединении к ней. В связи с чем, в настоящее время наша страна выступает в качестве наблюдателя, активно изучая возможности сотрудничества в области борьбы с киберпреступностью.

Кроме международных правовых документов, важную роль должны играть и национальные законодательства. Например, в США интернет-мошенничество относится к преступлению, регулируемому несколькими законодательными актами – Законом о борьбе с мошенничеством с использованием почты и электронных средств связи (Wire Fraud Act) и Законом о компьютерном мошенничестве и злоупотреблениях (Computer Fraud and Abuse Act)[9].

Вышеуказанные законы позволяют рассматривать уголовную ответственность лиц, совершающих интернет-мошенничество даже если жертвы находятся в другой стране.

В Казахстане же вопросы борьбы с интернет-мошенничеством рассматриваются Уголовным кодексом РК, который содержит нормы статьи, предусматривающие наказание за мошенничество, совершенное с использованием информационно-коммуникационных технологий.

Более того, учитывая растущую из года в год угрозу, исходящую от киберпреступности и распространения интернет-мошенничества, Глава государства Касым-Жомарт Токаев на расширенном заседании коллегии Министрерства внутренних дел РК 22 января 2024 года поручил профильному ведомству активизировать усилия в этом направлении, требуя от сотрудников полиции системного подхода и международного сотрудничества[10].

Реализацией данного поручения стали важные шаги в направлении усиления мер по защите населения от киберугроз путем:

- принятия Комплексного плана противодействия интернет-мошенничествам;

- создания в каждом территориальном Департаменте полиции специализированных подразделений «Киберпол»;

- блокирования в 2024 году свыше 8 тыс. мошеннических сайтов[11];

- создания на базе Национального банка РК антифрод-центров, которые играют важную роль в предотвращении вывода денежных средств за рубеж.

В рамках работы таких центров в Казахстане заблокировано более 400 млн тенге, которые мошенники пытались украсть у граждан[12].

Помимо этого, Казахстан активно сотрудничает с международными организациями, как в части обучения, так и в разработке новых механизмов борьбы с данным уголовным правонарушением.

Однако, несмотря на наличие международных и национальных законодательств, многие страны также, как и Казахстан сталкиваются с рядом трансграничных проблем, когда потерпевшие и преступники находятся в разных юрисдикциях, что усложняет привлечение виновных лиц к ответственности. Поскольку процесс экстрадиции и сотрудничества между правоохранительными органами разных стран может занимать значительное время и требовать затрат определенных ресурсов (например, материальных).

Рассматривая вопросы борьбы с киберпреступностью, следует также отметить такие проблемы, как сбор цифровых доказательств.

Данный вид преступления требует от правоохранительных органов применения специфических методов и инструментов для сбора доказательств, таких как лог-файлы в компьютерной системе или сетевых устройств, записи веб-серверов или электронные письма, транзакции, если это касается криптровалют или платежных систем и электронных денег.

И наиглавнейшую роль здесь играет такое направление деятельности правоохранительных органов, как цифровая криминалистика (форензика). Данная дисциплина регулирует вопросы выявления, сохранения и анализа цифровых следов, относящихся к делу.

На сегодняшний день, во многих странах

[9] *S.2864 – Computer Fraud and Abuse Act of 1984 // URL: https://www.congress.gov/bill/98th-congress/senate-bill/2864 (date of reference: 10.08.2024).*

[10] *О чем говорил Токаев на расширенном заседании коллегии МВД 22 января 2024 года // Bizmedia.kz // URL: https://bizmedia.kz/2024-01-22-o-chem-govoril-tokaev-na-rasshirennom-zasedanii-kollegii-mvd-22-yanvarya-2024-goda/?ysclid=m 1klusрпбz67426583 (дата обращения: 10.07.2024).*

[11] *Пострадавшим от кибермошенников казахстанцам возместили ущерб почти в 1 млрд тенге // Zakon.kz // URL: https://www.zakon.kz/sobytiia/6448262-postradavshim-ot-kibermoshennikov-kazak hstantsam-vozmestili-ushcherb-pochti-v-1-mlrd-tenge.html (дата обращения: 10.07.2024).*

[12] *S.2864 – Computer Fraud and Abuse Act of 1984 // URL: https://www.congress.gov/bill/98th-congress/senate-bill/2864 (date of reference: 10.08.2024).*

мира правоохранительные органы используют такие программы, как Hunchly или FTK Imager, которые позволяют следователям собирать цифровые доказательства из интернета, компьютерных систем и сетей.

В свою очередь данные компьютерные программы требуют специальной подготовки, наличие высококвалифицированных специалистов, обладающих знаниями в данной области.

Поэтому во многих странах правоохранительные органы разрабатывают специализированные учебные программы, создают учебные центры и проходят курсы подготовки. В этих программах уделяется внимание не только теоретическим, но и практическим аспектам.

Заключение

Таким образом, интернет-мошенничество, имеющее отношение к одному из подвидов киберпреступности, является одной из самых серьезных и растущих угроз в современном цифровом мире, как для граждан, организаций, так и государства в целом. Данный вид преступлений охватывает самый широкий спектр незаконных действий, которые используют преступники, начиная от фишинга до применения сложных финансовых схем с использованием криптовалют.

Все это требует от государства и правоохранительных органов, в частности, системного и комплексного подхода борьбы с интернет-мошенничеством, включая повышение профессионального уровня сотрудников правоохранительных органов через обучение в специализированных учебных заведениях (далее – СУЗ) правоохранительной направленности.

В частности, предлагается внедрить в программы обучения всех СУЗов предмет «Цифровая криминалистика», выделив ее как отдельную дисциплину из фундаментальной науки криминалистики, поскольку требует освоения технических методов работы с программным обеспечением.

Однако борьба с интернет-мошенничеством не должна быть только со стороны государства в лице уполномоченных государственных и правоохранительных органов, а также со стороны граждан, которые должны элементарно соблюдать кибергигиену, не допуская распространение вирусов и других вредоносных программ.

Наиболее эффективным способом противодействия интернет-мошенничествам должно стать повсеместное внедрение и использование таких современных технологий как блокчейн и работающий на опережение искусственный интеллект.

Применение этих технологий в сочетании с усилением законодательства, его правового регулирования и международного взаимодействия позволит значительно снизить количество преступлений данной категории, обеспечить защиту граждан в цифровом киберпространстве.

ЛИТЕРАТУРА

1. Jan Van Dijk: The Network Society. London: Sage Publications. 2012. // URL: https://www.researchgate.net/publication/298428268_Jan_Van_Dijk_The_Network_Society_London_Sage_Publications_2012 (date of reference: 02.09.2024).

2. 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. 10–14.

3. Атаманов, Р.С. Некоторые вопросы расследования мошенничества в сети Интернет // Актуальные проблемы российского права. – 2010. – № 4. – С. 201-205. // URL: https://cyberleninka.ru/article/n/nekotorye-voprosy-rassledovaniya-moshennichestva-v-seti-internet (дата обращения: 01.10.2024).

REFERENCES

1. Jan Van Dijk: The Network Society. London: Sage Publications. 2012. // URL: https://www.researchgate.net/publication/298428268_Jan_Van_Dijk_The_Network_Society_London_Sage_Publications_2012 (date of reference: 02.09.2024).

2. Abeuov D.A. Protivodejstvie kiberugrozam v Respublike Kazahstan. Problemy i puti reshenija na sovremennom jetape // «Habarshy — Vestnik» Karagandinskoj akademii MVD RK im. B. Bejsenova. — 2024. — № 4 (86). — S. 10–14.

3. Atamanov, R.S. Nekotorye voprosy rassledovanija moshennichestva v seti Internet // Aktual'nye problemy rossijskogo prava. – 2010. – № 4. – S. 201-205. // URL: https://cyberleninka.ru/article/n/nekotorye-voprosy-rassledovaniya-moshennichestva-v-seti-internet (data obrashhenija: 01.10.2024).