Министерство образования и науки Республики Казахстан

АО «Университет КАЗГЮУ имени М.С. Нарикбаева»

СЕРІК АЙНҰР СЕРІККЫЗЫ

Правовые основы предотвращения кибермошенничества: состояние и перспективы развития

образовательная программа 7М04208 - «Право IT»

Диссертация на соискание академической степени магистра права

Нур-Султан, 2022

Министерство образования и науки Республики Казахстан
АО «Университет КАЗГЮУ имени М.С. Нарикбаева»

«Допущен к защите»
Руководитель/координатор программы
_____
«__» _____ 20__ г.
_____

МАГИСТЕРСКИЙ ПРОЕКТ

На тему: «Правовые основы предотвращения кибермошенничества: состояние и перспективы развития»

по образовательной программе 7М04208 - «Право IT»

Выполнила **А. С. Серік**
Научный руководитель **Ph.D. Абай Абылайұлы**
Ph.D. О. В. Лозовая

Нур-Султан, 2022

УТВЕРЖДАЮ
Руководитель/координатор программы

_____
«__» _____ 20__ г.

Календарный план подготовки магистерского проекта

Наименование этапов проекта	Срок	отметка реализации этапов проекта			
		Фактический срок выполнения	Степень готовности выполненного этапа проекта	Подпись магистранта	Подпись научного руководителя
Осуществление обзора литературы и практических материалов	01.10. 2021	01.10.2021			
Разработка методологии	15.10. 2021	15.10.2021			
Сбор и обработка данных	30.01. 2022	30.01.2022			
Анализ и интерпретация полученных результатов	28.02. 2022	28.02.2022			
Разработка рекомендаций по проекту	15.03. 2022	15.03.2022			
Подготовка введения и заключения	01.04. 2022	01.04.2022			
Оформление диссертаций (проекта): Подготовка I раздела проекта	15.04. 2022	15.04.2022			
Подготовка II раздела проекта	01.05. 2022	01.05.2022			
Подготовка III раздела проекта	20.05. 2022	20.05.2022			

Получение отзыва научного руководителя (научных руководителей)	25.05. 2022	25.05.2022			
Подготовка доклада, наглядных пособий и презентации	14.06. 2022	14.06.2022			

Научный руководитель магистерского проекта

_____

(Абай Абылайұлы Ph.D., О. В. Лозовая Ph.D.)

План принял к исполнению:_____

(Серік А. С.)

Содержание

Список сокращений

РК – Республика Казахстан
КНР – Китайская Народная Республика
РФ – Российская Федерация
ФРГ – Федеративная Республика Германии
США – Соединенные Штаты Америки
СНГ – Содружество Независимых Государств
ООН - Организация Объединенных Наций
УК – Уголовный кодекс
МВД – Министерство внутренних дел
BEC – Business Email Compromise
EC3 – European Cybercrime Centre
IC3 – Internet Crime Complaint Center
IT – Information Technology
FBI – Federal Bureau of Investigation
IP – Internet Protocol
DNS – Domain name server

ВВЕДЕНИЕ

В век современных технологий и научно-технического прогресса появляются все больше новых видов преступлений. С 2020 года, когда мир впервые столкнулся с пандемией и локдаунами, Интернет вышел на пиковый спрос. Люди стали почти все время проводить в «онлайн» режиме, существенно выросло число преступлений в цифровом пространстве. При этом, многие из таких преступлений остаются безнаказанными, так как законодательство просто не успевает урегулировать новые правовые институты. Развитие общества в сторону цифровизации повлекло за собой новые формы преступления через информационные технологии. Компьютеры, мобильные телефоны, вредоносные программные обеспечения – все они являются средствами для осуществления киберпреступлений.

Одним из таких является цифровое мошенничество (оно же кибермошенничество, интернет-мошенничество и др.). Важность его правового регулирования состоит в том, что цифровое пространство стало нашей обычной частью жизни, в которой мы храним все самое важное, вплоть до денежных средств и банковских карт, конфиденциальных данных, переписок и личных вещей. Ввиду активизации злоумышленников в данной сфере и неготовности людей и правовых механизмов государств принять такие удары, пострадало много людей, компаний и даже государственных органов. Кибермошенничество является наиболее распространенным видом мошенничества, которое происходит на международном уровне. Цифровой мир стремительно развивался, при этом позволяя мошенникам взламывать личную и финансовую информацию людей различными способами. Мошенники уже могут использовать собранную информацию о пользователях, чтобы заполучить денежные средства. Поэтому важно, чтобы люди и организации знали, как защитить себя от кибермошенничества.

Большой прирост преступлений наблюдается не только в отношении физических лиц, но значительные убытки терпят и юридические лица. В связи с чем вопрос законодательного урегулирования правоотношений в цифровой среде, а также закрепления ответственности за преступления в цифровом пространстве, в частности за кибермошенничество, является особенно актуальным.

Актуальность темы исследования заключается в том, что ежегодный рост преступлений, совершаемых в киберпространстве приводит к масштабному изучению и способам предотвращения. В 2017 году в своем Послании «Третья модернизация Казахстана: Глобальная конкурентоспособность» отмечал Первый Президент Казахстана – Елбасы Н. Назарбаев в рамках защиты и обеспечения безопасности государства.

На данный момент проблема кибермошенничества стоит остро во всем мире. Для проведения различных махинаций мошенники стремятся максимально использовать уникальные возможности Интернета, такие как мгновенная рассылка электронных сообщений большому количеству адресатов или размещение информации на веб-сайте, так, что она становится доступна всему миру. «Пандемия COVID-19 продемонстрировала скорость, с которой преступные группы могут модифицировать свои методы, чтобы воспользоваться новыми возможностями для обмана отдельных лиц и компаний, ежедневно похищая миллионы долларов», — заявил генеральный секретарь Интерпола Юрген Шток[1]. Также на XI Конгрессе ООН по предупреждению преступности и уголовному правосудию, в рамках рассмотрения эффективных мер по предотвращению транснациональной организованной преступностью было уделено отдельное внимание преступлениям, которые совершаются с использованием информационных технологий[2]. Эксперты Организации Объединенных Наций также указывают на актуальность и значимость комплексного подхода в борьбе с киберпреступностью, как на законодательном уровне каждого государства-участника, таки в виде практических рекомендаций в техническом аспекте.

В последние годы количество интернет-мошенничества увеличивается, а методы совершенствуются, для хищения чужого имущества осуществляется без непосредственного контакта с лицом, кому принадлежат денежные средства. В этой связи создание рекомендаций по предотвращению компьютерных преступлений в нынешнее время одно из самых приоритетных направлений для международного сообщества. Рост и актуальность также отмечал Министр внутренних дел Республики Казахстана Ерлан Тургумбаев в казахстанско-французском форуме «Право в эпоху цифровых технологий»: «С развитием онлайн-услуг количество интернет-мошенничеств возросло в **2,3** раза. В этой связи, в структуре Центра по борьбе с киберпреступностью МВД созданы специальные группы, занимающиеся исключительно раскрытием этих преступлений»[3]. Однако, ссылаясь на ниже представленную статистику, исключительно

[1] 'INTERPOL Launches Centre Against Financial Crime And Corruption' (*Interpol.int*, 2022) <https://www.interpol.int/News-and-Events/News/2022/INTERPOL-launches-centre-against-financial-crime-and-corruption> accessed 14 March 2022

[2] 'Одиннадцатый Конгресс Организации Объединенных Наций По Предупреждению Преступности И Уголовному Правосудию' (Documents-dds-ny.un.org, 2022) <https://documents-dds-ny.un.org/doc/UNDOC/GEN/V05/822/61/PDF/V0582261.pdf?OpenElement> accessed 2 February 2022

[3] 'Опыт Цифровизации МВД Казахстана Вызвал Интерес У Зарубежных Экспертов' (*polisia.kz*, 2022) <https://polisia.kz/ru/opyt-tsifrovizatsii-mvd-kazahstana-vyzval-interes-u-zarubezhnyh-ekspertov/> accessed 2 May 2022

создание спец. групп не дает эффективной практики в расследовании и предотвращении киберпреступности в стране.

Цель исследования – анализ теоретических аспектов и разработка практических рекомендаций по совершенствованию правовых основ предотвращения кибермошенничества.

Задачи исследования:

- Провести комплексный анализ доктрины, судебной практики, и законодательства зарубежных стран в области мошенничества в киберпространстве;
- Изучить и определить пробелы в национальном законодательстве в сфере противодействия кибермошенничества;
- Ознакомиться и изучить лучшие практики по противодействию и расследованию кибермошенничества в зарубежных странах и на международном уровне;
- Разработать рекомендации по совершенствованию инструментов и методов предотвращения кибермошенничества.

Предмет исследования нормативно-правовая база и лучшая зарубежная практика.

Объект исследования правовые отношения публичного характера в рамках процесса предотвращения кибермошенничества.

Степень разработанности проблемы и теоретическая база исследования

На данную тему исследований небольшое количество. В ходе исследования были выделены следующие статьи: «Проблемы расследования киберпреступлений, которые стоят перед сотрудниками следственных органов» Нестерович Сергей Александрович, «Борьба с киберпреступлениями: сравнительный анализ законодательства стран СНГ» Джансараева Рима Еренатовна, Аратулы Куаныш, «Международно-правовая регламентация киберпреступности» Талипова Ляйсан Ринатовна. «Мошенничество в сети интернет» Ю.А. Стеценко, Н. С. Холодковская, «Система Правового Противодействия Финансовому Мошенничеству В России В Современных Условиях» Л.С. Хафизова.

Положения, выносимые на защиту

1. Имеющиеся в Уголовном кодексе состав преступления «мошенничество», который лишь подразумевает «кибермошенничество» как способ совершения, не позволяет в достаточной мере широко определять составы данного преступления. В связи с этим, существует значительная необходимость внесения изменений и дополнений в действующий уголовный кодекс Республики Казахстан. В частности, предлагается внесение статьи 190-1 в следующей редакции:

«**Кибермошенничество** – это хищение чужого имущества, приобретение права на чужое имущество путем обмана, злоупотребления доверием, а также ввода, изменения, удаления или блокирования компьютерных данных; или иного любого вмешательства в функционирование с использованием информационных сетей».

2. Для формирования верной правоприменительной практики при квалификации преступления «кибермошенничество» необходима качественная теоретическая проработка состава данного вида преступлений. В частности, особое внимание стоит уделить определению объекта и объективной стороны данного преступления, так как именно эти элементы отражают особый специфический характер данной категории преступлений.

3. Правовые основы предотвращения киберпреступлений часто не в полной мере обеспечивают цифровую безопасность в виду технических, организационных и других сопутствующих аспектов деятельности пользователей сети. Таким образом, необходимо: усилить контроль за безопасным использованием корпоративных локальных сетей и беспроводной связи государственным органам; усилить контроль по установке обязательных необходимых антивирусных программ; внедрить четкую систему отслеживания установки протоколов защиты на официальных сайтах организаций, а также на постоянной основе организовывать систематические курсы повышения квалификации для сотрудников правоохранительных органов в сфере цифровой криминалистики.

В качестве **базы источников исследования** также были использованы акты внутригосударственного (страны СНГ, Китай, США, Эстония, Германия и др.) и международного права (Конвенция Совета Европы о киберпреступности ETS № 185 (2001, Будапешт), Конвенция об обеспечении международной информационной безопасности (концепция, 2011), Таллинское руководство по применению международного права к кибероперациям, Проект ООН по всестороннему исследованию проблем киберпреступности, 2013), Резолюция Генеральной Ассамблеи 73/187 озаглавленной «Противодействие использованию информационно-коммуникационных технологий в преступных целях», а также Доклад Генерального секретаря ООН от 2019 года.

В Казахстане существует ряд нормативных актов, регулирующих информационное поле и закрепляют права человека на защиту от посягательств: Конституция Республики Казахстан, Уголовный кодекс Республики Казахстан, Кодексе Республики Казахстан "Об административных правонарушениях", законах Республики Казахстан "О государственных секретах", "О персональных данных и их защите", "Об электронном документе и электронной цифровой подписи", «Об

информатизации». В них были внесены дополнения и изменения в соответствии с разработанной Концепции кибербезопасности ("Киберщит Казахстана») от 30 июня 2017 года № 407, однако понятие «киберпреступление» отсутствует во всех нормативно правовых актов.

Практической базой исследования явились наиболее важные судебные решения Германии, США, Китая, стран СНГ.

Методы исследования

- Анализ и синтез – в данной работе присутствует анализ состояния кибермошенничества, рассматриваются основные проблемы, а также предлагаются пути решения.
- Формально-юридический (догматический) – заключается в исследовании норм национального и зарубежного законодательства.
- Дедукция – после изучения всеобъемливающего понятия преступления мошенничества был внесен новый состав исходя из специфики совершения с использованием информационных технологий.
- Сравнительно-правовой – заключается в сравнении норм законодательства зарубежных стран с нормами законодательства РК.

Научная новизна исследования заключается в том, что на сегодняшний день законодательство Республики Казахстан недостаточно охватывает составы преступлений в киберпространстве, в том числе мошенничество. Отсутствуют нормы в полной мере обеспечивающие ответственность, а также практические рекомендации для предотвращения кибермошенничества. Благодаря внесению самостоятельного состава, рекомендациям и курсам повышения квалификации в области цифровой криминалистики, сотрудники правоохранительных органов повысят качество расследований и рост раскрываемости такого вида преступления.

Практическая значимость исследования в том, что рекомендации по внесению в Уголовный кодекс Республики Казахстан нового состава преступления «кибермошенничество» разработанные в рамках диссертационной работы, могут быть применимы правоохранительными и уполномоченными органами в рамках исследуемой темы, а также судьями при уголовных делах, совершенных в киберпространстве.

Теоретическая значимость исследования выражается в том, что данная рекомендация будет полезна для учащихся как технических специальностей, таки юридических. Материалы диссертации могут использовать в государственных органах для обучения сотрудников от определения состава кибермошенничества до особенностей расследования цифровых преступлений.

Апробация результатов исследования

Результаты диссертационного исследования были включены в сборник «Инновационная юриспруденция: вопросы теории и практики: сборник

научных трудов по материалам II Международной научно-практической конференции студенческих научных объединений и молодых ученых 28 апреля 2022 г. - Тамбов, 2022».

Структура и объем диссертационного проекта

Работа состоит из введения, трех глав, восьми параграфов, заключения и библиографии.

РАЗДЕЛ 1. Теоретические основы определения кибермошенничества и способов предотвращения подобных преступлений.

1.1 Понятие и виды цифрового мошенничества. Способы совершения кибермошенничества.

Для начала стоит разобраться в том, что такое цифровое мошенничество. Законодательного закрепления данного понятия в странах СНГ – нет.

Уголовная ответственность за преступления в сфере компьютерных технологий предусмотрена главой 7 «Уголовные правонарушения в сфере информатизации и связи», а также существуют отдельные виды преступлений, которые совершаются с помощью компьютерных технологий, ярким примером является статья 190 – мошенничество, а именно п. 4, ч. 2 статьи 190 «путем обмана или злоупотребления доверием пользователя информационной системы».[4]

В Уголовном кодексе Республики Казахстан имеется определение понятия «мошенничество»:

«Мошенничество - хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием».

Максимальная санкция за данный вид преступления предусматривает лишение свободы от 5 до 10 лет с конфискации имущества с пожизненным лишением права занимать определенные должности или заниматься определенной деятельностью, а минимальная – штраф в размере до 1000 МРП, либо исправительные работы в том же размере, либо привлечение к общественным работам на срок до шестисот часов, либо ограничение свободы на срок до двух лет, либо лишение свободы на тот же срок, с конфискацией имущества.[5]

Основными составляющими мошенничества, как видно из диспозиции статьи 190 Уголовного Кодекса Республики Казахстан, является обман и злоупотребление доверием.

Обращаясь к толковому словарю Ожегова, обман – это то же, что и ложь, ложное представление о чем-либо, заблуждение.

Обман, согласно Комментарию к Уголовному кодексу Борчашвили И.Ш. (далее – Комментарий), бывает в отношении личности, имущества (прав на имущество), событий и действий, а также в намерениях.

При этом обман бывает двух видов: активный и пассивный. При активном обмане сообщается ложная или искаженная информация о чем-либо, при пассивном обмане происходит сокрытие информации о чем-либо.

---

[4] 'Уголовный Кодекс Республики Казахстан - ИПС "Әділет"' (*Adilet.zan.kz*, 2022) <https://adilet.zan.kz/rus/docs/K1400000226> accessed 28 April 2022

[5] 'Уголовный Кодекс Республики Казахстан - ИПС "Әділет"' (*Adilet.zan.kz*, 2022) <https://adilet.zan.kz/rus/docs/K1400000226> accessed 28 April 2022

«Злоупотребление доверием» состоит из двух основных слов, так, согласно толкового словаря Ожегова, злоупотребление – это проступок, состоящий в незаконном, преступном использовании своих прав, возможностей, а доверие – это уверенность в чьей-либо добросовестности и искренности[6].

Злоупотребление доверием, согласно Комментарию, это вид обмана, сопряженный с тем, что потерпевший доверяет и добровольно передает свое имущество (право на имущество)[7].

С учетом этого, стоит изучить множество вариантов словарных определений цифрового мошенничества:

В научной статье Красовской Н. Р., Гуляева А. А. кибермошенничество определяется как – активные действия в онлайн-формате с целью получения выгоды посредством манипуляций сознанием человека[8].

Цифровое мошенничество – это вид мошенничества в киберпространстве.

Согласно Кембриджскому словарю делового английского языка кибермошенничество – это ситуация, в которой кто-то использует Интернет для незаконного получения денег, товаров и т. д. от людей путем их обмана[9].

Цифровое мошенничество – это киберпреступление, основным умыслом которого является обман пользователей в цифровом пространстве с целью завладения их имуществом.

Кибермошенничество – это преступление, совершенное с помощью компьютера с намерением испортить личную и финансовую информацию другого человека, хранящуюся в Интернете[10].

Цифровое мошенничество – это попытка хищения имущества пользователей путем обмана с помощью современных технологий.

---

[6] 'ЗЛОУПОТРЕБЛЕНИЕ Толковый Словарь Ожегова Онлайн' (*Slovarozhegova.ru*, 2022) <https://slovarozhegova.ru/word.php?wordid=9249> accessed 17 February 2022

[7] 'Комментарий К Уголовному Кодексу Республики Казахстан (Особенная Часть)' (Zakon.uchet.kz, 2022) <https://zakon.uchet.kz/rus/docs/T9700167_1_> accessed 2 May 2022

[8] Красовская Наталия Рудольфовна, Гуляев Андрей Анатольевич 'К ВОПРОСУ О КИБЕРМОШЕННИЧЕСТВЕ' (*КиберЛенинка*, 2022) <https://cyberleninka.ru/article/n/k-voprosu-o-kibermoshennichestve> accessed 28 April 2022

[9] 'Cyberfraud' (*Dictionary.cambridge.org*, 2022) <https://dictionary.cambridge.org/ru/%D1%81%D0%BB%D0%BE%D0%B2%D0%B0%D1%80%D1%8C/%D0%B0%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9/cyberfraud> accessed 28 April 2022

[10] 'What Is Cyber Fraud? - Deltanet' (DeltaNet, 2022) <https://www.delta-net.com/knowledge-base/compliance/fraud-awareness/what-is-cyber-fraud/> accessed 18 May 2022

Цифровое мошенничество делится на разные виды, в иностранных источниках они представлены следующими терминами:

«Scam, con, swindle, extortion, sham, double-cross, hoax, cheat, ploy, ruse, hoodwink, confidence trick».

При этом, существует множество видов и способов совершения цифрового мошенничества:

Фишинг (англ. phishing, от fishing — рыбная ловля, выуживание и password — пароль) — вид интернет-мошенничества, цель которого — получить идентификационные данные пользователей. Сюда относятся кражи паролей, номеров кредитных карт, банковских счетов и другой конфиденциальной информации[11]. Фишинг реализовывают через фиктивные сообщения на электронную почту, мессенджеры и всплывающие уведомления. В большинстве случаев мошенники преследуют финансовый интерес, поэтому маскируются под банковские организации, провайдеров и системы электронных платежей для получения доступа к онлайн-банкингу или кошельку жертвы для вывода денежных средств. Схема работает таким образом, что лица, получают электронное фишинг-письмо с просьбой перейти на веб-сайт, обновить систему или направить ответ для подтверждения личности. Мошенники действуют достаточно грамотно и убедительно, что практически невозможно отличить поддельное письмо. Как правило преступники создают идентичный веб-сайт на короткое время, где запрашивают конфиденциальную информацию. Например, сайт банка, где нужно ввести свой логин и пароль, номер телефона, данные кредитных карт, PIN-код и код доступа (если таковое имеется) и вот уже ваши данные на руках у злоумышленников, которые вы предоставили сами. Для этого они используют методы социальной инженерии, придумывая различные ситуации, например, угрозы блокировки банковской карты без подтверждения личности, либо сообщают о взломе аккаунта и предоставляют фишинговую ссылку для авторизации.

Фишинг эволюционировал и теперь имеет несколько разновидностей, использующих аналогичные методы: **вишинг, смишинг и фарминг**. **Вишинг** (англ. Vishing, от voice – голос +phishing) – одна из разновидностей фишинга, реализуется методами социальной инженерии с помощью телефонного звонка. На телефон атакуемого поступает звонок, и злоумышленник различными способами выуживает все необходимые данные для реализации умысла. Еще одним видом является **смишинг** (англ. Smishing, от sms – служба коротких сообщений +phishing) реализуется с помощью рассылки через СМС – сообщения с вредоносной ссылкой, зачастую это оповещения о выигрыше какого-либо приза. В текстовом

[11] 'Что Такое “Фишинг”' (*Encyclopedia.kaspersky.ru*, 2022) <https://encyclopedia.kaspersky.ru/knowledge/what-is-phishing/> accessed 28 April 2022

сообщении указывается поздравительный текст и ссылка для получения гарантированного приза. Осведомленность пользователей про фишинговые атаки с каждым разом растет, в связи с этим хакеры создали новый метод – **фарминг**. Технически фарминг сложнее в реализации, так как посредством кэша DNS-серверов (серверы доменных имен) и вируса программного обеспечения перенаправляют с легитимного веб-сайта на сторонние страницы с поддельными доменами и IP-адресами без ведома пользователя, что также приводит к краже данных. Распознать фарминг труднее, так как замена сайтов происходит незаметно и если не обратить на этот факт внимание, то все имеющиеся данные окажутся в уязвимом положении.[12]

Компрометация деловой электронной почты (BEC). Ключевым элементом в совершении данного мошенничества является фишинг/спуфинг. При BEC-атаке злоумышленники получают доступ к корпоративным сетям, далее могут рассылать различные электронные письма сотрудникам от имени компаний, поставщиков, с которыми они сотрудничают и производят оплату зачастую безналичным способом. Здесь могут применяться как методы социальной инженерии, таки технический взлом компьютеров. Центр жалоб на интернет-преступления (IC3) ФБР сообщает, что мошенничество с BEC было самой дорогой из кибератак в 2020 году: было подано 19369 жалоб и скорректированные убытки в размере около 1,8 миллиарда долларов, а также 71% организаций признали, что они были свидетелями атак с целью компрометации деловой почты[13].

Нигерийские письма или мошенничество «419». Еще один вид цифрового мошенничества, при котором злоумышленники присылают письма о якобы полученном вами наследстве, для которого необходимо всего-то оплатить доставку или что-то еще и для этого требуются данные карты. Также довольно распространённая схема такого мошенничества – вывоз денежных средств «чиновником» с Нигерии. Злоумышленники, выдавая себя за чиновника предлагают процент от переводимых сумм, которые выплатят после незаконного перевода или переезда чиновника. Жертвы предоставляют свою конфиденциальную информацию: номера банковских счетов, бланки, которые в последствии используются для вывода средств с их счетов. Несмотря на то что, казалось бы, никто не поведется на «письма счастья» ежегодно убытки достигают миллионы долларов. Особо доверчивых заманивали в Нигерию, где в результате они были заключены в

[12] 'Фишинг, Вишинг, Смишинг, Фарминг — В Чем Разница' (*Protectimus.com*, 2022) <https://www.protectimus.com/blog/ru-phishing-vishing-smishing-pharming/> accessed 28 April 2022

[13] Antipov A, 'Лучшие Методы Предотвращения Атак Компрометации Деловой Электронной Почты (BEC)' (*Securitylab.ru*, 2022) <https://www.securitylab.ru/blog/personal/bezmaly/351180.php> accessed 28 April 2022

тюрьму, так как Правительство Нигерии не сочувствуют своим жертвам, поскольку жертва буквально вступает в сговор в незаконном переводе, которое противоречит законодательству данного государства. Название такого вида мошенничества исходит из статьи 419 Уголовного кодекса Нигерии о мошенничестве, который конкретно касается людей, обращающихся за помощью в переводе денег, через электронную почту[14].

Также существуют другие виды кибермошенничества, например, **проведение псевдолотерей и конкурсов** – для такого вида мошенничества, как правило пользователя просят заполнить регистрационную форму для получения данных; **инвестиционные схемы, проекты и финансовые пирамиды** – быстрые и легкие деньги с красивой рекламой, на которые ведутся множество людей, добровольно переводя деньги на счета злоумышленников, после чего те или пропадают, или блокируют «жертв»; **письма в социальных сетях и рассылки** – после взлома социальных сетей, всем друзьям пользователя приходит сообщение с просьбой одолжить денег или оплатить лечение кому-то из его близких и номер карты, после чего злоумышленник пропадает, а пользователь возвращает доступ к странице себе; **фальшивые интернет-магазины –** со времен пандемии множество людей стали заказывать все необходимое в интернете, в связи с чем на ряду с нормальными интернет-магазинами, появились фальшивые, которые сложно отличить. После перевода денег за товар вы окажетесь в черном списке или вас просто будут игнорировать. Тем самым, злоумышленник получит ваши денежные средства от вас добровольно. В интернет-магазинах всегда нужно смотреть настоящие ли там отзывы, живая ли страничка, а лучше брать только у проверенных или спрашивать о таких у своих знакомых; **фальшивые платежные системы** – никогда не стоит оплачивать что-то в интернете через свою кредитную карту на непроверенных сайтах и через незнакомые платежные системы. Злоумышленники получают полный доступ к вашей карте, так как вы самостоятельно вводите все данные карты; **программы-вымогатели** – это один из типов вредоносного ПО, которыми пользуются мошенники для вымогательства денежных средств путем удержания данных или блокировки устройств через электронные письма или USB-накопителя, с целью получения выкупа. Примерно таким же образом и мотивом осуществляется **отказ в обслуживании**, для вымогания денежных средств.

Данный список пополняется каждый день новыми видами кибермошенничества и все перечислить невозможно, поэтому мы раскрыли самый распространённый вид мошенничества в отношении физических лиц

[14] 'Welcome To FBI.Gov | Federal Bureau Of Investigation' (*Federal Bureau of Investigation,* 2022) <https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/nigerian-letter-or-419-fraud> accessed 2 May 2022

(фишинг), мошенничество, направленное на юридических лиц (компрометация деловой электронной почты) наносит большой финансовый ущерб, а также Нигерийские письма, за которые могут привлечь уголовную ответственность за содействие в совершении преступления.

Чтобы оценить масштабность проблемы цифрового мошенничества, стоит рассмотреть статистические данные. Так, согласно статистике, в Республике Казахстан в 2021 году количество фактов цифрового мошенничества составило 17800, что в 2 раза выше показателей 2019 года. Самыми «атакуемыми» оказались город Нур-Султан, Алматы, Карагандинская, Костанайская и Восточно-Казахстанская области. Говоря о способах, самыми распространенными оказались получение денежных средств за товар или услугу на сайтах, предназначенных для размещения объявлений (8,2 тысячи случаев), благодаря получению конфиденциальной информации, мошенникам удалось оформить 2,7 тысячи микрокредитных займов на людей, вишинг также не остался в стороне и составил 2,3 тысячи случаев, «выгодные» предложения о легком заработке и вложениях составили 1,9 тысяч случаев, фишинг и фальшивые ссылки – 1,3 тысячи случаев[15]. Мошенничество растет пропорционально вместе с количеством пользователей в сети, которые активно попадаются на уловки злоумышленников. Это также наглядно показывает отсутствие кибергигиены и осведомленности населения.

Международный опыт Малайзии, Сингапура, Великобритании, Германии, Чехии, Франции, Литвы, Эстонии, Финляндии, Швеции и Швейцарии был изучен при разработке концепции кибербезопасности, т.е. проекта «Киберщит Казахстана». Целью Концепции является достижение и поддержание уровня защищенности электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры от внешних и внутренних угроз, обеспечение устойчивого развития Республики Казахстан в условиях глобальной конкуренции. Срок реализации концепции состоит из двух этапов. Будут пересмотрены образовательные программы и профессиональные стандарты для увеличения количества и качества подготовки специалистов в области информационной безопасности. Будет обеспечено повышение квалификации действующих сотрудников, работающих в данной сфере, а также налажена эффективная схема взаимодействия и сотрудничества промышленности и науки в развитии отечественных разработок[16].

---

[15] 'Названы Распространенные Схемы Кибермошенничества' (*Деловой портал Капитал.кз,* 2022) <https://kapital.kz/gosudarstvo/100440/nazvany-rasprostranennyye-skhemy-kibermoshennichestva.html> accessed 28 April 2022

[16] Об утверждении Концепции кибербезопасности ("Киберщит Казахстана")

1.2 Основные принципы и направления предупреждения и расследования преступлений кибермошенничества.

Так как киберпреступления являются транснациональной разновидностью преступлений. В целом совершить киберпреступление достаточно легко, для этого не нужно физическое присутствие и деяние совершается очень быстро. Существуют технические проблемы: отслеживание IP-адреса преступника (ов), так как в сети можно зашифровать адрес, также уязвимость программных обеспечений, через которые совершаются противоправные деяния, в последствии происходит утечка данных, посягательство на права человека. Правовые затруднения могут быть вызваны установкой факта совершения преступления, лица или группу лиц, совершивших преступление, вопросы юрисдикции, определение способа и мотива преступления и так далее. Как показывает практика, наличие лишь юридического образования не дает эффективного результата в расследовании и предотвращении преступлений в киберпространстве[17].

Свыше тысячи киберпреступлений зарегистрировано в Казахстане с начала года. При этом раскрываемость таких преступлений не превышает и 3%[18]. Это доказывает отсутствие знаний у сотрудников правоохранительных органов в области юриспруденции и IT технологий, что значительно затрудняет процесс предотвращения преступлений и привлечения к ответственности за них. К примеру, Е. С. Шевченко отметил, что ряде регионов России был проведен опрос среди следователей, который показал следующие результаты: у 95% опрошенных имеется только юридическое образование и 5% следователей дополнительно получили образование по специальности «Информатика и вычислительная техника». Большинство отметили недостаточность знаний для расследования киберпреступлений, в том числе мошенничества[19].

В целом совершить интернет-мошенничество достаточно легко, для этого не нужно физическое присутствие и деяние совершается очень быстро. Существуют следующие проблемы расследования:

Постановление Правительства Республики Казахстан от 30 июня 2017 года № 407 https://adilet.zan.kz/rus/docs/P1700000407

[17] Серік А. С. контрольная работа в рамках курса «Цифровая криминалистика».

[18] Inbusiness.kz. 2022. Раскрываемость киберпреступлений в Казахстане не превышает 3%. [online] Available at: <https://inbusiness.kz/ru/news/raskryvaemost-kiberprestuplenij-v-kazahstane-ne-prevyshaet-3> [Accessed 10 April 2022].

[19] Studbooks. 2022. Использование специальных познаний при расследовании мошенничества в сфере компьютерной информации. [online] Available at: <https://studbooks.net/2427202/pravo/ispolzovanie_spetsialnyh_poznaniy_rassledovanii_moshennichestva_sfere_kompyuternoy_informatsii> [Accessed 10 April 2022].

- Трансграничный характер преступления: из-за отсутствия каких-либо территориальных границ преступник может находиться в любой точке мира. Сложность расследования заключается в необходимости правоохранительным органам доступа и обмена данными, охвате большого количества людей.
- Существуют технические проблемы: процесс подборки методов для нахождения следов; сохранение и анализ цифровых доказательств, на которых достаточно легко «оставить цифровой след» или повредить; отслеживание IP-адреса преступника (ов); уязвимость программных обеспечений, через которые совершаются противоправные деяния, в том числе происходит утечка данных, посягательство на права человека.
- Правовые затруднения могут быть вызваны квалификацией, установкой факта совершения преступления, лица или группу лиц, совершивших преступление, определение способа и мотива преступления, определение методов применимых правоохранительными органами для расследования, латентность преступления, пробелы в законодательстве и так далее.

По статистическим данным Комитета по правовой статистике и специальным учетам при Генеральной прокуратуре Республики Казахстан в период с 2016 года по 2020 год несмотря на снижение общей преступности, количество совершаемых киберпреступлений возросло в 51 раз (с 117 до 5968 уголовных правонарушений в год). Показательной является раскрываемость таких преступлений: с начала 2020 года органами внутренних дел страны зарегистрировано 8 337 дел о мошенничествах, совершенных в отношении пользователей информационных систем. Из указанного числа раскрыто 1709 дел, около 5000 остаются нераскрытыми, а уже в 2021 году всего за три месяца три месяца 2021 органами внутренних дел зарегистрировано 6824 таких преступлений[20].

Преступники не только злоупотребляют методом социальной инженерии, но и обладают специальными знаниями в области информационных технологий, с каждым разом совершенствуя способы совершения преступных деяний, что может отражаться в профессиональном сокрытии следов. Раскрытие данного вида преступления полностью зависит от планирования и координации следственных действий, направленных на обнаружение и фиксацию электронных следов преступления. В первую очередь входе осуществления предварительного расследования при

[20] profit.kz. 2022. Интернет-мошенничество в Казахстане: тысячи таких дел остаются не раскрытыми. [online] Available at: <https://profit.kz/news/58861/Internet-moshennichestvo-v-Kazahstane-tisyachi-takih-del-ostautsya-ne-raskritimi/> [Accessed 21 April 2022].

совершении мошенничеств с использованием интернет-ресурсов необходимо провести следующие следственные действия:

- Принятие заявления о совершении правонарушения и формирование следственно-оперативной группы для проведения дальнейших оперативно-розыскных действий с учетом специфики кибермошенничества.
- Определение тактики: в какой последовательности будут проходить процессуальные действия, какие методы будут применяться исходя из специфики совершения преступления.
- Определение «места» совершения преступления: одно из самых затруднительных аспектов в расследовании это – трансграничный характер преступления. На данном этапе определяется нахождение устройства, при помощи IP-адреса, посредством которого совершены противоправные деяния. Во многих случаях злоумышленники используют разные техники сокрытия действительного адреса, используют зарубежные серверы.
- Осмотр объекта – данный этап важен для установления конкретной техники, которым было совершено противоправное деяние. Совместно со следственной группой могут быть привлечены незаинтересованные эксперты с техническими знаниями. Осмотр требует особой аккуратности, для сохранности и чистоты следов.
- Допрос свидетеля и назначение экспертизы являются завершающим этапом, по результатам которой выносится заключение. Исходя из способа совершения кибермошенничества могут назначаться компьютерные, экономические или криминалистические экспертизы.

Успешное расследование любого вида преступления, кроется в умении определять не только уголовно-правовую составляющую, но криминалистическую сущность. Следы преступления составляют особо значимые криминалистические данные в расследовании. В трудах авторов приводятся различные классификации, так, например, Коломинов В. В. предлагает два вида классификации следов мошенничества: традиционные следы (следы пальцев рук на компьютере, и др. техники), компьютерные следы (которые остаются в памяти устройства при любых действиях с компьютерными или иными программируемыми устройствами)[21]. Из этого стоит сделать вывод о том, что нет как исчерпывающих способов

[21] Dslib.net. 2022. Расследование мошенничества в сфере компьютерной информации: научно-теоретическая основа и прикладные аспекты первоначального этапа. [online] Available at: <http://www.dslib.net/finans-pravo/rassledovanie-moshennichestva-v-sfere-kompjuternoj-informacii-nauchno-teoreticheskaja.html> [Accessed 10 April 2022].

совершения мошенничества, таки методов по расследованию и к каждому отдельному нужен индивидуальный подход.

Вопросы об изучении различных методов и поисков действующих механизмов в расследовании кибермошенничества поднимают ученные из разных стран. Например, кандидат юридических наук Хафизова отмечала два направления в борьбе с киберпреступностью: 1) максимально эффективное предупреждение, профилактика, предотвращение самой возможности правонарушений; 2) ориентация на выявление, пресечение и раскрытие совершенных преступных деяний[22]. Большой шаг в продвижении цифровой криминалистики в своих трудах отмечают Марк Баттон, Бранислав Хок и Дэвид Шеперд, которые предлагают ввести дисциплину специализирующиеся именно на расследовании экономических преступлениях[23]. Только принятые меры в совокупности могут дать эффективный результат в предотвращении финансового мошенничества. Необходимо отметить значимость повышения квалификации сотрудников органов внутренних дел, обучения в зарубежных странах для изучения позитивного опыта передовых государств в расследовании кибермошенничества, укрепления международного сотрудничества для расследования преступления с трансграничным характером. Немаловажную роль играет информирование населения для оказания содействия в раскрытии интернет-преступлений, что в дальнейшем непосредственно приведёт к заметному снижению киберпреступности. Криминалистические знания в сфере информационных технологий требуют комплексного подхода в разрешении имеющихся проблем, которые подтверждаются статистикой, научной позицией и судебными делами.

[22] Л.С. Хафизова, 'Система Правового Противодействия Финансовому Мошенничеству В России В Современных Условиях' (КиберЛенинка, 2022) <https://cyberleninka.ru/article/n/sistema-pravovogo-protivodeystviya-finansovomu-moshennichestvu-v-rossii-v-sovremennyh-usloviyah> accessed 5 January 2022

[23] Button M, Hock B, and Shepherd D, Economic Crime From Conception to Response (1st edn, Published April 25, 2022 by Routledge, 314 p.)

РАЗДЕЛ 2. Анализ опыта зарубежных государств и международного права в сфере предотвращения преступлений мошенничества в киберпространстве.

Пандемия COVID-19 внесла свою лепту в мир киберпреступлений во всем мире. Достаточно большой показатель финансового ущерба наблюдался за последние три года. Злоумышленники применяют новые инструменты адаптируя их под конкретную ситуацию: мониторинг новостных порталов, нововведений в здравоохранении и экономике вовремя локдауна создали почву для преступлений в сфере информационных технологий. Все чаще гражданам приходили электронные письма с предложением покупки дефицитных лекарств и вакцин от короновируса, средств медицинского характера, как маски, антисептики, а также приглашения для участия в специальном конкурсе вакцинированных граждан. Все эти письма содержали в себе форму для заполнения данных для подтверждения личности, если требовалось данные банковских счетов, которые были в последствии были использованы мошенниками.

Чем же отличаются киберпреступления от традиционного понятия?

На первый взгляд кажется, что только использованием компьютера, однако для совершения мошенничества не всегда нужно компьютерное устройство. Преступники создают «тело» в цифровом пространстве, которые состоят из различных идентификационных чисел и хранятся в базе данных провайдеров. Перемещаясь и меняя устройства виртуальное «тело» также локацию и сетевые данные. Киберпространство в целом достаточно обширная по своему понятию, это больше, чем простой телефонный разговор, или переписка. Интернет как глобальная сеть, которая охватывает каждую точку планеты, интернет предлагает злоумышленникам гибкость в укрытии. Можно провести параллель с традиционным преступлением, в виртуальном пространстве можно оставить цифровые следы, точно также как следы от обуви в реальной жизни. Для отслеживания различных противоправных деяний необходимо ратифицировать международные договоры, охватывающие киберпреступления. Одним из таких международных договоров является Конвенция о компьютерных преступлениях (Конвенция Совета Европы о киберпреступности, Convention on Cybercrime CETS № 185) (Будапешт, 23 ноября 2001 года). Данная конвенция является самым первым международным договором о преступлениях, совершенных через Интернет и другие компьютерные сети, и касается, в частности, нарушений авторских прав, компьютерных мошенничеств, детской порнографии и нарушений безопасности сети. Она также содержит ряд полномочий и процедур, таких как обыск

компьютерных сетей и перехват[24]. Отталкиваясь из актуальности проблемы государства предпринимают различные методы и правовые инструменты для предотвращения.

2.1 Законодательство и практика в сфере киберпреступлений США.

США является одной из первых стран, которая ввела уголовную ответственность за совершение интернет мошенничество. По данным отчета специального подразделения ФБР – Центра жалоб на преступления в Интернете (Internet Crime Complaint Center) в 2021 кибермошенники причинили ущерб в размере 6,9 миллиарда долларов. В IC3 поступило 847376 жалоб, что на 7% больше, чем в предыдущем году. Большая часть жалоб касались компроментации деловой почты, а также различных случаев кибервымогательства[25]. Если ссылаться на цифры, то на фишинг (в том числе на фарминг, вишинг и смишинг) поступило 323 972 жалоб с ущербом в 44,213,707 долларов США, 19 954 потерпевших от BEC-атак, а общий ущерб исчисляется в 2,395,953,296 долларов США[26]. В списке по количеству обращений и убытков лидирует штат Калифорния.

В США есть как федеральные, таки законы отдельных штатов криминализирующие различные виды преступлений, связанные с компьютерными системами, в том числе мошенничество с использованием информационных технологий. Так, согласно 18 Своду законов США глава 47 , которое именуется как «Мошенничество и ложные заявления» включает в себя § 1343 охватывающую мошенничество, совершенное с использованием электронных средств связи, а также электронной почты и Интернета, в качестве уголовной ответственности лицу, разработавшему или намеревающемуся разработать какую-либо схему для обмана или получения денежных средств посредством мошеннических действий через радио, телевизионной или проводной связи с целью выполнения мошенничества грозит лишение свободы на срок до 20 лет. Если такое же деяние совершается в период объявленным президентом чрезвычайной ситуацией или затрагивает финансовые учреждения, наказание может увеличиться до 30 лет лишения свободы и/или штрафом в размере до 1

[24]'Киберпреступность (Будапештская Конвенция)' (*Воздействие Европейской конвенции о правах человека*, 2022) <https://www.coe.int/ru/web/impact-convention-human-rights/convention-on-cybercrime#/Sweden> accessed 2 May 2022

[25] 'Ущерб От Деятельности Интернет-Мошенников В США Достиг Рекордных $6,9 Млрд — ФБР | Digital Russia' (*Digital Russia*, 2022) <https://d-russia.ru/ushherb-ot-dejatelnosti-internet-moshennikov-v-ssha-dostig-rekordnyh-6-9-mlrd-fbr.html> accessed 2 May 2022

[26]'Internet Crime Report 2021' (*Ic3.gov*, 2022) <https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf> accessed 2 May 2022

миллиона долларов[27]. В соответствии с данным законом для привлечения к ответственности достаточно отправки электронного письма. Также можно привлечь к уголовной ответственности по следующим статьям: § 1028 «Мошенничество и связанная с ним деятельность в отношении к документам, удостоверяющими личность, функциями аутентификации и информацией», § 1029 «Мошенничество и связанные с ним действия в отношении устройств доступа», § 1030 «Мошенничество и связанные с ним действия в отношении компьютеров».

Как отмечалось ранее, во всех штатах существуют законы, устанавливающие ответственность за преступления, совершенные с помощью компьютерных технологий. Некоторые из них напрямую касаются конкретных видов кибермошенничества: фишинг, отказ в обслуживании, программы-вымогатели и другие.

В штате **Коннектикут** Уголовный кодекс применяет практику разделения по классам, например, «Телефонное мошенничество первой степени: уголовное преступление класса B» предусматривает ответственность за преступление, когда лицо (1) сознательно или преднамеренно разрабатывает или участвует в схеме, направленной на выманивание у другого лица денег или имущества, (2) (A) использует ложные отговорки или ложные обещания, независимо от стоимости, получает денежные средства или имущество путем вымогательства, и (3) использует телефонный звонок, включая, помимо прочего, звонок, сделанный физическим лицом, автоматический телефонный звонок и записанное сообщение, для получения таких денег или имущества от такого другого лица[28]. Различие по классам основываются в денежном эквиваленте. В классе «B» если превышает двадцать тысяч долларов, в классе «C» превышает десять тысяч долларов, в классе «D» две тысячи долларов.

Уголовным кодексом штата **Флориды** – лицо, совершившее или имеющие намерение совершить мошеннические действия с использованием идентифицирующей информацией другого лица, косвенно представляя себя другим лицом посредствам веб-страницы, домена в Интернете без разрешения или одобрения такого другого лица, отсылает или связывает получателя сообщения с веб-страницей прямо или косвенно побуждает, просит или просит получателя сообщения электронной почты предоставить идентифицирующую информацию несет наказание в соответствии с

[27] '18 U.S. Code § 1343 - Fraud By Wire, Radio, Or Television' (*LII / Legal Information Institute*, 2022) <https://www.law.cornell.edu/uscode/text/18/1343> accessed 2 May 2022

[28] 'Chapter 952 - Penal Code: Offenses' (*Cga.ct.gov*, 2022) <https://www.cga.ct.gov/current/pub/chap_952.htm#sec_53a-125c> accessed 2 May 2022

законодательством штата[29]. К данной статье можно отнести такие мошенничества, как фишинг, смишинг, фарминг, вишинг, компрометацию деловой почты, где злоумышленники под именем других лиц получают персональные данные жертвы.

Уголовный кодекс штата **Мичиган**, §750.409b, раздел 777.16t предусматривает наказания за несанкционированное владение или использование программ-вымогателей[30].

В **Северной Дакоте** ответственность о сообщении попыток киберпреступлений также возлагают на организации. Уголовный Кодекс § 54.59.1-01 – 54-59.1-07 требует, чтобы организация сообщила в отдел о выявленном или предполагаемом инциденте угрожающую кибербезопасности, который влияет на конфиденциальность, целостность или доступность информационных систем, данных или услуг. Раскрытие информации должно быть сделано в максимально возможное время и без необоснованных задержек[31]. Несмотря на лидерство США в сфере законотворчества, пока даже уполномоченные государственные органы страны признают, что победа со спамом продолжается, в силу чего в США постоянно совершенствуют собственное законодательство[32]. Тем самым, можно заметить, что правоохранительным органам нужно постоянная модернизация в борьбе с цифровыми экономическими преступлениями, так как с каждым пользователем информационных технологий, растет и количество угроз.

2.2 Законодательство и практика в сфере киберпреступлений Китая.

Преступления в сфере информационных технологий попадают под регулирование нормативных актов Китайской Народной Республики и с ежегодным развитием информатизации приобретают актуальность и значение. В Китае существуют органы, которые регулируют и отвечают за расследование и предотвращение киберпреступлений:

---

[29] 'Statutes & Constitution :View Statutes : Online Sunshine' (*Leg.state.fl.us*, 2022) <http://www.leg.state.fl.us/STATUTES/index.cfm?App_mode=Display_Statute&Search_String=&URL=0600-0699/0668/Sections/0668.703.html> accessed 2 May 2022

[30] 'Michigan Computer Laws § 750.409B' (*Casetext.com*, 2022) <https://casetext.com/statute/michigan-compiled-laws/chapter-750-michigan-penal-code/subchapter-miscellaneous/section-750409b-ransomware-possession-use-prohibition-violation-as-felony-penalty-ransomware-defined> accessed 23 May 2022

[31] 'North Dakota Century Code T54c59.1' (*Ndlegis.gov*, 2022) <https://ndlegis.gov/cencode/t54c59-1.pdf#nameddest=54-59p1-06> accessed 2 May 2022

[32] Погорелова М. А. , 'Правовое Регулирование Распространения Информации В Сети Интернет В Условиях Глобализации' (*Cyberleninka.ru*, 2022) <https://cyberleninka.ru/article/n/pravovoe-regulirovanie-rasprostraneniya-informatsii-v-seti-internet-v-usloviyah-globalizatsii/viewer> accessed 8 January 2022

Министерство общественной безопасности (MPS) – отвечает за признание киберпреступлений, например, за неправомерное использование Интернета для воровства, мошенничества и вымогательства;

Министерство промышленности и информационных технологий (MIIT) (Департамент политики, законов и нормативных актов) является одним из основных учреждений, участвующих в текущей правовой реформе с 1996 года, а в 2008 году был создан центр, отвечающий за прием обращений и сообщений о кибермошенничестве, фишинговых сообщениях содержащие в себе вирусы или незаконную информацию, которая может привести к утечке конфиденциальных данных.

Интернет-общество Китая (ISC) – в 2004 году был основан специальный центр сообщения о незаконной информации в Интернете (CIIRC), который принимает жалобы через веб-сайт www.net.china.cn о противоправных действиях в сети, тем самым оказывают помощь правоохранительным и административным органам в борьбе с киберпреступлениями, продвигают и разрабатывают инициативы по общественному просвещению в отношении законов об Интернете и этике в Интернете, а также сотрудничают с международными партнерами и содействуют усилиям по решению проблем, вызывающих общую обеспокоенность в отношении глобальной сети, на международной арене[33].

Статья 287 Уголовного кодекса Китайской Народной Республики (14 марта 1997 года) закрепляет следующее: «Любой, кто использует компьютер для финансового **мошенничества**, кражи, коррупции, незаконного присвоения государственных средств, кражи государственных секретов или других преступлений, должен быть осужден и наказан в соответствии с соответствующими положениями этого закона»[34]. А также в Постановлении «О телекоммуникациях» в Разделе 161 «Доступ к компьютеру с преступными или недобросовестными намерениями» закрепляется положение о том, что лицо, получивший незаконный доступ к компьютеру с намерением обмануть и совершить преступление наказывается лишением свободы до 5 лет. А также ответственность за поддержание безопасности Интернета лежит на провайдере, и нарушения со стороны пользователей приведут к аннулированию бизнес-лицензии провайдера и его регистрации в сети, штрафам и возможному уголовному преследованию как сотрудников компании, так и пользователей. Это способствует

[33] 'Reporting And Policing Internet Crimes In China' (*Hg.org*, 2022) <https://www.hg.org/legal-articles/reporting-and-policing-internet-crimes-in-china-22958> accessed 2 May 2022

[34] 'Criminal Law Of The People's Republic Of China' (Cybercrimelaw.net, 2022) <https://www.cybercrimelaw.net/China.html> accessed 2 May 2022

снижению рисков осуществления противоправных деяний в киберпространстве.

Правоохранительные органы в Китае активно предпринимают меры против киберпреступлений, направленные на нарушение личных данных, хакерские атаки, препятствующие на нормальное функционирование компьютеров, кибермошенничество и на другие правонарушения в Интернете. Также вносят лепту в поддержании кибербезопасности, так они ответили на более чем 1000 запросов о помощи в расследовании и предоставлении информации от Интерпола, установили каналы взаимной судебной помощи и двусторонние каналы сотрудничества с правоохранительными органами более 70 стран и регионов[35].

2.3 Сравнительный анализ правовых основ предотвращения киберпреступлений стран СНГ.

Законодательство **Российской Федерации** закрепляет положения об ответственности лиц, совершивших киберпреступления. Также, как и в Уголовном кодексе Республики Казахстан в Российской Федерации есть глава 28 «***Преступления в области компьютерной информации***», которая включает в себя такие статьи, как: статья 272 «Неправомерный доступ к компьютерной информации», статья 273 «Изготовление, использование и распространение вредоносных программ для электронных вычислительных машин», статья 274 «Нарушение правил эксплуатации ЭВМ, системы или сети». За интернет мошенничество, как отдельный вид преступления, ответственность предусмотрена главой 21 «***Преступления против собственности***», в разделе преступлений в сфере экономики. Статья 159.3. закрепляет мошенничество с использованием электронных средств платежа, а статья 159.6. мошенничество в сфере компьютерной информации.

П. 1 статьи 159.6 отражается следующим образом: «Мошенничество в сфере компьютерной информации, то есть хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей – наказывается штрафом в размере до ста двадцати тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года, либо обязательными работами на срок до трехсот шестидесяти часов, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо арестом на срок до

[35]'Cybercrime In China' (*Unodc.org,* 2022) <https://www.unodc.org/documents/Cybercrime/English.pdf> accessed 3 May 2022

четырех месяцев»[36]. Статья 159.3 закрепляет «Мошенничество с использованием электронных средств платежа», согласно п.19 статьи 3 Федерального закона от 27.06.2011 N 161-ФЗ (ред. от 02.07.2021) "О национальной платежной системе" Российской Федерации: «электронное средство платежа - средство и (или) способ, позволяющие клиенту оператора по переводу денежных средств составлять, удостоверять и передавать распоряжения в целях осуществления перевода денежных средств в рамках применяемых форм безналичных расчетов с использованием информационно-коммуникационных технологий, электронных носителей информации, в том числе платежных карт, а также иных технических устройств»[37].

Как отмечалось раннее, пандемия спровоцировала резкий скачок киберпреступности и Россия не исключение. Рост произошел исключительно за счет телефонного и интернет-мошенничества, по сравнению с первым полугодием 2019 года, в 2020 году число потерпевших от рук «белых воротничков» выросло на 76%[38]. Из-за того, что вовремя локдауна население изолировалось и вся деятельность перешла на онлайн формат, количество традиционных преступлений значительно сократилось.

По данным СберБанка, мошенники, которые ежемесячно крадут со счетов граждан посредством телефонных звонков от 3,5 млрд до 5 млрд. рублей, а общий ущерб банка составил более 60 млрд рублей. По официальной статистике МВД РФ за восемь месяцев 2021 г. в совокупности возбуждено 385 000 дел в сфере кибермошенничества[39].

Результаты исследования Национального агентства финансовых исследований (НАФИ) показали следующее: За 2021 каждый десятый россиянин (11%) – сталкивался с мошенничеством в сфере интернет-покупок, 7% из них понесли финансовые потери в результате действий

---

[36] УК РФ Статья 159.6. Мошенничество В Сфере Компьютерной Информации \ Консультантплюс (*Consultant.ru*, 2022) <http://www.consultant.ru/document/cons_doc_LAW_10699/51c53d82b60ac8c009745bdea3838d507064c6d3/> accessed 3 May 2022

[37] 'О Национальной Платежной Системе От 27 Июня 2011 - Docs.Cntd.Ru' (Docs.cntd.ru, 2022) <https://docs.cntd.ru/document/902286143> accessed 13 April 2022

[38] 'Эксперты Назвали Самый Популярный Способ Мошенничества В Интернете' (rbc.ru, 2022) <https://www.rbc.ru/technology_and_media/09/02/2021/602184e19a794726a2165b6b> accessed 10 April 2022

[39] 'Почему Киберпреступления – Угроза Национальной Безопасности' (Ведомости, 2022) <https://www.vedomosti.ru/technology/articles/2021/12/07/899278-kiberprestupleniya-bezopasnosti> accessed 11 May 2022

преступников, а 4% смогли вернуть свои деньги[40]. Довольно внушительные результаты среди населения. Немаловажный факт, что интернет-шоппинг может приобретать различные виды мошенничества от поддельных сайтов с умышленным искажением домена, например, вместо https://wildberries.ru отправить на лже-сайт https://wildberriess.ru, либо на этих самых сайтах продавать товары, выдавая себя продавцами, вариаций достаточное количество, что предугадать какой-то определенный способ совершения достаточно тяжело. НАФИ также провели опрос среди населения, кем же должна производиться борба с кибермошенничеством: 11% россиян склоняются к тому, что люди должны сами проявлять бдительность и осторожность, сохраняя кибергигену; 61% придерживаются того мнения, чтобы предотвращением интернет мошенничества должны заниматься правоохранительные органы и при совершении преступных деяний расследовать их; 13% возлагают ответственность на провайдеров и организаций, в основном такого мнения придерживаются более молодое поколение[41].

В современной России интернет мошенничество – это целая индустрия, которая постоянно развивается и совершенствуется, во многом благодаря откровенной безнаказанности[42]. Тем не менее Россия предпринимает меры по раскрытию и предотвращению такого вида преступлений. Например, власти создали органы по борьбе с киберпреступностью: ГосСОПКА (государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы России) под руководством ФСБ, ФинЦЕРТ (Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере), Управление «К» при МВД РФ, а также другие дополнительные спецподразделения по раскрытию и расследованию преступлений в сфере информационных технологий[43].

Уголовный кодекс **Украины** в статье 190 закрепляет мошенничество, совершенное в крупных размерах, или путем незаконных операций с использованием электронно-вычислительной техники и предусматривает

---

[40] 'Каждый Десятый Россиянин Сталкивался С Продавцами-Мошенниками В Интернете — НАФИ' (Nafi.ru, 2022) <https://nafi.ru/analytics/kazhdyy-desyatyy-rossiyanin-stalkivalsya-s-prodavtsami-moshennikami-v-internete/> accessed 3 May 2022

[41] 'Каждый Десятый Россиянин Сталкивался С Продавцами-Мошенниками В Интернете — НАФИ' (Nafi.ru, 2022) <https://nafi.ru/analytics/kazhdyy-desyatyy-rossiyanin-stalkivalsya-s-prodavtsami-moshennikami-v-internete/> accessed 3 May 2022

[42] Комаров А.А. Криминологическая экспертиза некоторых законопроектов, связанных с Интернетом //Современное право. - 2009. - №6. - С. 109-113.

[43] 'Почему Киберпреступления – Угроза Национальной Безопасности' (*Ведомости*, 2022) <https://www.vedomosti.ru/technology/articles/2021/12/07/899278-kiberprestupleniya-bezopasnosti> accessed 11 May 2022

ответственность в виде лишения свободы на срок от трех до восьми лет[44]. Также в Разделе 16 закрепляются преступления, совершенные с использованием электронно-вычислительных машин, их систем или сетей.

Около 70% жалоб и обращений, поступающих в киберполицию Украины, составляет мошеннические действия в информационном пространстве. На состояние за 2021 год сотрудники правоохранительных органов направили в суд более чем двух тысяч уголовных дел[45]. В Украине самыми распространёнными видами мошенничества являются фишинг, псевдо-лотереи и конкурсы, фиктивные интернет-магазины, а также просьбы о благотворительности.

Как отмечалось раннее, мошенники используют методы социальной инженерии и быстро адаптируются под различные ситуации. Злоумышленники не прошли мимо нестабильного политического положения в Украине. Под предлогом социальных выплат гражданам и переселенцам, преступники рассылают фишинговые сообщения с ссылкой на сайт, в котором нужно заполнить заявку и авторизоваться. Для зачисления денежных средств нужно предоставить персональные данные и реквизиты банковских карт, которые в дальнейшем перейдут во владение злоумышленников.[46] Украинцы на почве военных действий попадаются на уловки благотворительного мошенничества, перечисляя денежные средства на карты преступников; сталкиваются с объявлениями о заказе фальшивых документов для перевода через границу мужчин призывного возраста. На что были предупреждены об уголовной ответственности не только мошенников, которые в дальнейшем не выдадут документы после оплаты, но и самих граждан изъявивших желание заказать их[47].

---

[44] 'Преступления Против Собственности : Уголовный Кодекс Украины : Уголовный Кодекс : Кодексы Украины : Недвижимость Украины - Meget.Kiev.Ua' (2022) <https://meget.kiev.ua/kodeks/ugolovniy-kodeks/razdel-1-6/> accessed 3 May 2022

[45] 'В Прошлом Году В Украине Активизировались Интернет-Мошенники. В НБУ Рассказали, По Каким Схемам Они Работают | Громадское Телевидение' (*Hromadske.ua*, 2022) <https://hromadske.ua/ru/posts/v-proshlom-godu-v-ukraine-aktivizirovalis-internet-moshenniki-v-nbu-rasskazali-po-kakim-shemam-oni-rabotayut> accessed 3 May 2022

[46] 'Мошенники Выманивают Деньги В Украинцев Под Видом Помощи Переселенцам - Полиция' (Ukrinform.ru, 2022) <https://www.ukrinform.ru/rubric-society/3462308-mosenniki-vymanivaut-dengi-u-ukraincev-pod-vidom-pomosi-pereselencam-policia.html> accessed 25 April 2022

[47] 'Киберполиция Рассказала Об Основных Мошеннических «Схемах» В Условиях Военного Положения' (Ukrinform.ru, 2022) <https://www.ukrinform.ru/rubric-society/3449782-kiberpolicia-rasskazala-ob-osnovnyh-mosenniceskih-shemah-v-usloviah-voennogo-polozenia.html> accessed 3 May 2022

Министр внутренних дел Украины Арсен Аваков заявил в ходе онлайн-конференции «Цифровая трансформация государства: перспективы и риски кибербезопасности» о том, что Киберполиция Украины в целях повышения продуктивности и качества в противодействии преступлений в информационном поле ведет набор компетентных специалистов с соответствующими знаниями в данной области[48]. Такое решение поднимет раскрываемость преступлений, а также сыграет большую роль в противодействии, в том числе и мошенничества.

Украина активно занимается реализацией государственной политикой в сфере противодействия киберпреступности, заблаговременно информируя и внедряя специальные программы для систематизации и пресечения преступности в информационном поле.

В феврале 2009 года Парламентом **Республики Молдовы** был ратифицирована Конвенция о киберпреступности (ETS N 185), принятая в Будапеште 23 ноября 2001 года, в том же году был одобрен Закон о предотвращении и борьбе с преступностью в сфере компьютерной информации. Данный Закон регулирует вопросы предотвращения киберпреступности, защиты и оказания помощи пользователям информационных систем, сотрудничества и взаимопомощи органов государственного управления в сфере кибербезопасности[49]. К Конвенции присоединились 62 страны-участницы, в том числе и страны из постсоветского пространства: Азербайджан, Армения, Украина, Грузия и неродственно сама Республика Молдова. Также в статусе наблюдателей входят 14 государств.

Также в Уголовном кодексе Молдовы появилась глава XI «Информационные преступления и преступления в области электросвязи», которая включает в себя 10 статей, устанавливающих ответственность за эту разновидность уголовно-наказуемых деяний, в том числе за кибермошенничество. Статья 260_6 «**Информационное мошенничество**» звучит в следующей редакции: «Ввод, изменение или удаление информационных данных, ограничение доступа к этим данным или иные способы препятствования функционированию информационной системы с целью извлечения материальной выгоды для себя или иного лица, если эти

[48] 'МВД: Киберполиция Украины Переходит На Новый Уровень Работы И Объявляет Большой Набор Специалистов - ITC.Ua' (ITC.ua, 2022) <https://itc.ua/news/mvd-kiberpolicziya-ukrainy-perehodit-na-novyj-uroven-raboty-i-obyavlyaet-bolshoj-nabor-speczialistov/> accessed 7 April 2022

[49] 'ЗАКОН Республики Молдовы № 20 От 03.02.2009 По Предотвращению И Борьбе С Киберпреступностью' (Legis.md, 2022) <https://www.legis.md/cautare/getResults?doc_id=12742&lang=ro> accessed 17 May 2022

действия повлекли причинение ущерба в крупных размерах наказываются штрафом в размере от 1350 до 1850 условных единиц, или неоплачиваемым трудом в пользу общества на срок от 150 до 200 часов, или лишением свободы на срок от 2 до 5 лет»[50]. То есть в Молдове ответственность за мошенничество предусматривается не в главе против собственности, а в отдельной, которая предусматривает именно информационные преступления.

Основными уполномоченными органами в области предупреждения и борьбы с киберпреступностью являются:

Министерство внутренних дел – проводят специальные розыскные мероприятия, уголовное преследование, международное сотрудничество, а также идентифицируют киберпрестуаников. Существует также *Служба информации и безопасности*, которая базируется на вопросах предотвращения и противодействия киберпреступности, предоставляющей угрозу национальной безопасности государству. Вместе с этим в рамках своих компетенций могут проводить розыскные мероприятия и принимает меры по выявлению преступных организаций в информационном мире. Данная служба сотрудничает с *Министерством экономики и инфраструктуры*, которые представляют предложения по обеспечению защиты информационных данных[51].

Генеральная прокуратура – осуществляет уголовное преследование, координирование и руководство над судопроизводством. В 2016 году была создана *Прокуратура по борьбе с организованной преступностью и особым делам*, в компетенции которой проводить уголовные преследования по информационным преступлениям, в случае превышения ущерба 50 тысяч единиц[52].

Правоохранительные органы Республики Молдовы отмечают мошенничество, как одну из самых больших рисков на компании и на общую экономическую «погоду». В связи с этим они собирают команды реагирования в составе которых есть опытные следователи, эксперты по финансовым и компьютерным экспертизам направленные на борьбу с компьютерным мошенничеством.

---

[50] 'Уголовный Кодекс Республики Молдовы' (*Legislationline.org*, 2022) <https://www.legislationline.org/download/id/10026/file/MOLD_CC_2021_ru.pdf> accessed 23 May 2022

[51] Николайчук А, 'Обзор Законодательства Молдовы: Борьба С Киберпреступностью' (*Digital Report*, 2022) <https://digital.report/zakonodatelstvo-moldovy-infobezopasnost-9/> accessed 14 May 2022

[52] Николайчук А, 'Обзор Законодательства Молдовы: Борьба С Киберпреступностью' (*Digital Report*, 2022) <https://digital.report/zakonodatelstvo-moldovy-infobezopasnost-9/> accessed 14 May 2022

2.4 Опыт предотвращения киберпреступлений Европейских стран.

Федеральное правительство **Германии** объявило направление кибербезопасности главным приоритетом, так как сбои и не урегулирование сферы IT могут оказать влияние на внутреннюю безопасность. Большое внимание на данный вопрос уделяет Федеральное министерство внутренних дел, который 9 ноября 2016 года принял «Стратегию кибербезопасности». Все последующие обновления в данную Стратегию содержат цели и меры на повышение безопасности в киберпространстве[53]. Государство обеспечивает и оценивает все процессы изменений, нововведений в целях регулирования правоотношений без ущерба и формирования базовых условий.

Уголовный кодекс **Федеративной Республики Германии** широко охватывает положения материального права в соответствии с Будапештской конвенции о киберпреступности. Компьютерное мошенничество закрепляется в статье 263a: «лицо, с намерением получить незаконную материальную выгоду для себя или для третьего лица, нанося ущерб имуществу другого лица, влияя на результат операции обработки данных путем неправильной настройки компьютерной программы, использования неверных, неполных или получением несанкционированных данных». Также предусмотрена ответственность в соответствии с пунктом 1 для лиц, которые совершают преступления путем создания компьютерных программ или закупает такие программы, владеет ими или поставляет их для третьих лиц – наказывается лишением свободы на срок до трех лет или денежным штрафом[54]. Как и во многих государствах и в Германии положения компьютерного мошенничества закреплены отдельным составом в главе 22 «Мошенничество и растрата». Статьи данной главы были включены в связи с возрастающей киберпреступностью с целью закрытия пробелов законодательстве. Так как Германия является страной-участницей Будапештской конвенции о киберпреступности, политика предотвращения

[53] 'IT & Cyber-Sicherheit' (*Bundesministerium des Innern und für Heimat*, 2022) <https://www.bmi.bund.de/DE/themen/it-und-digitalpolitik/it-und-cybersicherheit/it-und-cybersicherheit-node.html;jsessionid=B5FDE9BF4B544D519A20DBC7860E9E12.1_cid364> accessed 8 March 2022

[54] 'German Criminal Code (Criminal Code In The Version Published On 13 November 1998 (Federal Law Gazette I, P. 3322), As Last Amended By Article 2 Of The Act Of 19 June 2019 (Federal Law Gazette I, P. 844))' (Legislationline.org, 2022) <https://www.legislationline.org/download/id/10003/file/GERM_CC_en.pdf> accessed 7 April 2022

преступлений в цифровом пространстве соответствует положениям конвенции, а также на основании этого разработаны Стратегии.

Вместе со стратегией ФМВД разработали законопроект «О кибербезопасности» с целью улучшения IT безопасности и защиты пользователей сети. Согласно законопроекту, были предложены поправки в действующие законы, например, в Закон о телекоммуникациях, Закон о защите данных и в ряд других, касающийся критически важных информационных структур. Ответственный подход к цифровизации отразились на принятии соответствующих специальных норм: «Закон об интернет-услугах (Telemediengesetz-TMD)», «Закон о Федеральном управлении по информационной безопасности», «Второй закон о повышении безопасности систем информационных технологий (Закон о безопасности ИТ 2.0)»[55]. Отдельное внимание уделили обязанности юридических лиц о сообщении об инцидентах и нарушениях безопасности сетей.

Немаловажным является Закон «О международной взаимной помощи по уголовным делам». Германия осуществляет не только внутреннюю политику по предотвращению и расследованию киберпреступности, но и как участник многих договоров и конвенций о международном судебном сотрудничестве в рамках Европейского Союза и Совета Европы оказывает содействие государствам. Германия также входит в Совместную целевую группу по борьбе с киберпреступностью (J-CAT) Центра киберпреступности Европола (EC3) для дальнейшего усиления борьбы с киберпреступностью в Европейском Союзе и за его пределами. Данную инициативу поддержали ряд других государств: Австрия, Канада, Германия, Нидерланды, Италия, Франция, Испания, Великобритания и США. Колумбия и Австралия.

Глава Европейского центра киберпреступности Троэльс Эртинг комментирует: «Цель состоит в том, чтобы предотвратить киберпреступность, сорвать ее, поймать мошенников и забрать их незаконную прибыль. Это первый шаг на долгом пути к открытому, прозрачному, бесплатному, но в то же время безопасному Интернету. Эта цель не может быть достигнута силами правоохранительных органов в

[55] 'Cybercrime Policies/Strategies In Germany' (Octopus Cybercrime Community, 2022) <https://www.coe.int/en/web/octopus/country-wiki-ap/-/asset_publisher/CmDb7M4RGb4Z/content/germany/pop_up?_101_INSTANCE_CmDb7M4RGb4Z_viewMode=print&_101_INSTANCE_CmDb7M4RGb4Z_languageId=en_GB> accessed 7 April 2022

одиночку»[56]. Вместе с международным сотрудничеством Германия предпринимает меры и внутри государства. Были созданы специальные учреждения: Оперативное управление государственной уголовной полиции (Landeskriminalamt-LKA), а при активном росте преступлений в цифровом пространстве формировать Центр по борьбе с киберпреступностью; Федеральное ведомство уголовной полиции осуществляет координацию международного контакта с полицией и уполномочен расследовать особо тяжкие киберпреступления; также существуют подразделения в прокуратуре, с 2011 года функционирует Национальный центр киберзащиты[57]. В мире происходит продвижение в принятии мер по предотвращению противоправных деяний во всемирной паутине и принятие участие государств в таких инициативах только усилит внутреннюю политику, которая положительно повлияет на сокращение киберинцидентов.

Глава 14 Уголовного кодекса **Эстонии** закрепляет «Преступления в сфере компьютерной информации и обработки данных», несмотря на наличие отдельной статьи «Мошенничество» статья 268 выделяет отдельный состав «Компьютерное мошенничество». Согласно диспозиции компьютерное мошенничество – это получение чужого имущества, имущественной либо иной выгоды путем ввода компьютерных программ или информации, их модификации, уничтожения, блокирования либо иного вида вмешательства в процесс обработки информации, влияющего на результат обработки информации и обусловливающего причинение прямого имущественного или иного вреда собственности другого лица, - наказывается штрафом, или арестом, или лишением свободы на срок от одного года до шести лет[58]. Также, как и во всем мире в 2020 году в период пандемии возросло количество кибермошенничества, которые реализовывались различными методами. Например, веб-констебль (это

[56] 'Expert International Cybercrime Taskforce Is Launched To Tackle Online Crime | Europol' (Europol, 2022) <https://www.europol.europa.eu/media-press/newsroom/news/expert-international-cybercrime-taskforce-launched-to-tackle-online-crime-0> accessed 8 February 2022

[57]'Cybercrime Policies/Strategies In Germany' (Octopus Cybercrime Community, 2022) <https://www.coe.int/en/web/octopus/country-wiki-ap/-/asset_publisher/CmDb7M4RGb4Z/content/germany/pop_up?_101_INSTANCE_CmDb7M4RGb4Z_viewMode=print&_101_INSTANCE_CmDb7M4RGb4Z_languageId=en_GB> accessed 7 April 2022

[58]'Уголовный Кодекс Эстонии' (Legislationline.org, 2022) <https://www.legislationline.org/download/id/6462/file/Estonia_CC_as_of_2002_ru.pdf> accessed 7 May 2022

сотрудники местной полиции, которые работают в социальных сетях)[59] Маарья Пунак отмечала новые виды интернет мошенничества связанные с рассылкой фишинговых писем о вакцинации от Департамента здоровья, тем самым играя и давя на страхи людей. Также она отмечала важность раскрытия не личность преступников, а пресекать их деяния. А ведущий аналитик RIA (Департамент государственной инфосистемы) Лаури Танклер указала на невозможность проверки на существование той или иной организации, с которой были наложены сотруднические взаимоотношения в связи с ограничением передвижения[60]. Тенденция проведения мошеннических схем играя на общественном страхе наблюдается во всем мире.

Департаментом государственной инфосистемы (RIA) в июне 2020 года было зарегистрировано 276 инцидентов, мошенники использовали данные эстонцев из регистра гос. закупок, так после получения информации о тендере Ида-Таллиннской центральной больницы, которое выиграло литовское предприятие, злоумышленники связывались с больницей от имени организации и в результате выманили обманным путем 10000 евро[61].

Наравне с распространёнными видами мошенничества любовные аферы случаются довольно часто. В сравнении со схемой «звонок от банка» от которого мошенники могут получить около 17 тысяч евро, в то время как от «любовного мошенничества» ущерб может составить около 15 тысяч евро, несмотря на значительно меньшее количество совершения, ущерб стоит наряду с инвестиционным мошенничеством[62]. Зачастую это происходит таким образом, что лица знакомятся через Интернет, после общения возлюбленная просит отправить денежные средства на покупку билета и бронирование отеля для того что бы прилететь к жертве, однако после перевода страницы удаляются и пользователь отправляется в блок.

---

[59] 'Веб-Констебли' (Juristaitab.ee, 2022) <https://www.juristaitab.ee/ru/chabo/veb-konstebli> accessed 7 May 2022

[60] 'Самые Популярные Виды Мошенничества В Эстонии И Как Государство Задерживает Иностранных Киберпреступников' (www.gloss.ee, 2022) <https://www.gloss.ee/2020/11/11/samye-populyarnye-vidy-moshennichestva-v-estonii-i-kak-gosudarstvo-zaderzhivaet-inostrannyh-kiberprestupnikov/> accessed 9 May 2022

[61] 'Кибермошенники Стали Использовать Данные Из Регистра Госзакупок' (*ERR*, 2022) <https://rus.err.ee/1120167/kibermoshenniki-stali-ispolzovat-dannye-iz-registra-goszakupok> accessed 11 May 2022

[62] 'Опасный Tinder И "Любовные Мошенничества": Какими Способами В 2021 Году У Жителей Эстонии Выманили 10 Млн Евро?' (*Delfi RUS*, 2022) <https://rus.delfi.ee/statja/95621501/opasnyy-tinder-i-lyubovnye-moshennichestva-kakimi-sposobami-v-2021-godu-u-zhiteley-estonii-vymanili-10-mln-evro> accessed 6 May 2022

Правительство Эстонии проводят профилактические действия по кибербезопасности как для жителей, таки для правоохранительных органов. Например, Департамент государственной инфосистемы (RIA) организовывает учебные семинары для госслужащих, сотрудников объекта жизнеобеспечения и местного самоуправления; составляют рекомендации для предупреждения и предотвращения киберпреступлений, в том числе мошенничества; сотрудники проходят тестирования для проверки знаний по кибербезопасности[63]. Такие курсы повышения квалификации и осведомленности граждан помогает значительно улучшить состояние киберпреступности.

Структура полиции состоит из двух ветвей – одна из них Центральная Криминальная Полиция (ЦКП), которая осуществляет функции центрального органа Эстонии по борьбе с различными формами организованной преступности, в частности с серьезными экономическими преступлениями и преступлениями в сфере информационных технологий. ЦКП проводит судебные экспертизы и технические исследования, что способствует расследованию и предотвращению интернет мошенничества, принимает участие в следственных действиях.

Большим преимуществом является взаимодействие с Интерполом, Европолом и Шенгенской информационной системой, а также сотрудничает с зарубежными правоохранительными органами[64]. Например, в 2020 году ЦКП задержал преступников из Румынии, которые на протяжении полутра лет через различные веб-сайты пытались получить неправомерный доступ к банковским счетам людей и паролям Smart-ID[65].

Эстонская политика в противодействии киберпреступлениям, в частности кибермошенничества на практике показывает положительные результаты сотрудничества с международным сообществом.

---

[63] 'Профилактика И Рекомендации | Riigi Infosüsteemi Amet' (Ria.ee, 2022) <https://www.ria.ee/ru/kiberbezopasnost/profilaktika-i-rekomendacii.html> accessed 5 May 2022

[64] 'Полиция Эстонской Республики' (*Eurasialaw.ru*, 2022) <https://eurasialaw.ru/nashi-rubriki/politsiya-gosudarstv-mira/politsiya-estonskoj-respubliki> accessed 12 May 2022

[65] 'Мошенники Коронавирусного Времени — Что Следует Знать И Как Защититься' (*Tribuna.ee*, 2022) <https://tribuna.ee/tribuna/crime/novye-vidy-moshennichestva-estonia/> accessed 8 May 2022

РАЗДЕЛ 3. Перспективы развития механизмов предотвращения преступления мошенничества с применением информационных технологий в Республике Казахстан.

3.1 Изменения и дополнения в действующее уголовное законодательство.

Стремительное развитие цифровизации повлияло и на Республику Казахстан. Ежегодный рост киберпреступлений вызывает общественный резонанс, в особенности – мошенничество. Большое разнообразие методов, способов совершения и распространённость данного вида преступления требует отдельного внимания. Про это отмечал Президент Республики Казахстан в своем послании, а также был поднят вопрос на межведомственной комиссии по профилактике правонарушений под председательством премьер-министра РК Аскара Мамина рассмотрены вопросы противодействия интернет-мошенничеству[66]. Изучение и адаптация законодательства под преступления с использованием информационно – коммуникативных систем является актуальным в нынешних реалиях. Несмотря на наличие п.4 ч.2 статьи 190 в Уголовном кодексе Республики Казахстан, она не охватывает в полной мере специфику преступления.

Кибермошенничество включает в себя широкий перечень преступлений в киберпросторанстве. Например, это может быть кража персональных данных и выражаться в фишинге, может быть взлом корпоративного или личного компьютера посредством рассылки спам-писем, с дальнейшим требованием выкупа, а также ввод, изменение данных в неправомерных целях. То есть при квалификации интернет-мошенничества зачастую касаются и смежные составы, такие как «**Статья 207. Нарушение работы информационной системы или сетей телекоммуникаций**», «**Статья 208. Неправомерное завладение информацией**» и другие статьи Уголовного кодекса.

Вопрос о вынесении Интернет мошенничества отдельным составом преступления стоит достаточно давно. Так, исследователи высказывали необходимость введения отдельной нормы. Например, Т. Тропина придерживается той позиции, что различные манипуляции с компьютерными данными, которые в последствии приводят к завладению права на чужое имущество и чужим имуществом нельзя квалифицировать по статьям 158 «Кража» и 159 «Мошенничество» Уголовного кодекса

[66] 'Вдвое Выросло Количество Интернет-Мошенничеств В Казахстане' (*profit.kz*, 2022) <https://profit.kz/news/62084/Vdvoe-viroslo-kolichestvo-internet-moshennichestv-v-Kazahstane/> accessed 1 April 2022

Российской Федерации[67], а также указывает на противоречие одному из базовых уголовно-правовых принципов «nullum crimen, nulla poena sine lege – нет преступления без указания о нем в законе»[68] в случае применения на практике квалификаций по совокупности. Также автор отмечает, что дополнение в статью «Мошенничество» действий с использованием компьютерных технологий, не решит проблемы при квалификации преступлений с использованием информационных технологий[69].

Профессор Б.В. Волженкин провёл анализ Уголовного кодекса Федеративной Республики Германии и наряду с основным составом мошенничества, также предусматривают разновидность компьютерного мошенничества: «Законодатель, вероятно, выделил компьютерное мошенничество в самостоятельный состав преступления, имея в виду необычность способа совершения преступления с использованием компьютерной техники, когда в «заблуждение» вводится электронно-вычислительная машина, так как ответственность предусматривалась идентичная»[70]. То есть в целом, передовые государства области цифровизации поддерживаются позиции введения отдельного состава, который предусматривает ответственность за хищение имущества в информационном поле.

Модернизация законодательства в сфере компьютерных преступлений является ключевым звеном в сокращении таких противоправных деяний. Ульрих Зибер[71] выделял 6 основополагающих этапа в формировании законодательства в сфере компьютерных преступлений:

- защита данных и защита неприкосновенности частной жизни;
- уголовное законодательство о борьбе с экономическими преступлениями, связанными с использованием компьютеров;

---

[67] '"Уголовный Кодекс Российской Федерации" (УК РФ) От 13.06.1996 N 63-ФЗ (Последняя Редакция) \ Консультантплюс' (*Consultant.ru,* 2022) <http://www.consultant.ru/document/cons_doc_LAW_10699/> accessed 11 May 2022

[68] Тихонравов Е, 'Принцип Nullum Crimen Sine Lege В Истории Отечественного Уголовного Права' (Cyberleninka.ru, 2022) <https://cyberleninka.ru/article/n/printsip-nullum-crimen-sine-lege-v-istorii-otechestvennogo-ugolovnogo-prava/viewer> accessed 16 April 2022

[69] 'FRAUD IN THE INTERNET: CRIMINOLOGICAL CHARACTERISTICS AND QUALIFICATION PROBLEMS' (*Cyberleninka.ru,* 2022) <https://cyberleninka.ru/article/n/moshennichestvo-v-seti-internet-kriminologicheskaya-harakteristika-i-problemy-kvalifikatsii/viewer> accessed 21 April 2022

[70] Волженкин Б. В. Мошенничество: Серия «Современные стандарты в уголовном праве и уголовном процессе». СПб., 1998. 36 с. (21 с.)

[71] Прим. Ульрих Зибер - немецкий юрист, профессор права, директор Института зарубежного и международного уголовного права им. М. Планка, Германия, Фрайбург.

- защита интеллектуальной собственности;
- защита от противозаконного и вредного контента;
- уголовно-процессуальное законодательство;
- правовое регулирование защитных мер, таких как криптография и требования в отношении аутентификации[72].

Есть ряд элементов, которые необходимо учесть при решении проблем в сфере цифровой преступности: обеспечить закрепление определений в законе, законодательно закрепить полномочия по ведению расследования в целях борьбы с киберпреступностью, а также обеспечить осуществление этих полномочий в рамках соблюдения основополагающих прав и свобод человека[73]. Принятие положений в национальное законодательство в первую очередь в интересах государств для обеспечения экономической и социальной безопасности. Стремительное масштабирование словно вирус киберпреступности наносит значительный ущерб не только физическим и юридическим лицам, а также государству в целом.

Для усовершенствования законодательства Республики Казахстан существует значительная необходимость внесения изменений и дополнений в действующий уголовный кодекс Республики Казахстан. В частности, предлагается внесение статьи **190-1** в следующей редакции:

«1. ***Кибермошенничество*** – это хищение чужого имущества или приобретение права на чужое имущество путем обмана, злоупотребления доверием, а также ввода, изменения, удаления или блокирования компьютерных данных; или иного любого вмешательства в функционирование компьютерной системы с использованием информационных сетей[74],-

В соответствии с данной статьей необходимо предусмотреть санкции исходя из отягчающих обстоятельств, если деяние:

1) совершенное группой лиц по предварительному сговору;

2) лицом с использованием своего служебного положения;

---

[72] 'A Comparative Study Of Cybercrime In Criminal Law: China, US, England, Singapore And The Council Of Europe' (*Repub.eur.nl*, 2022) <https://repub.eur.nl/pub/94604/PROOF-Qianyun-Wang-BW-1-.pdf> accessed 1 March 2022

[73] A/CONF.203/14 O, 'Одиннадцатый Конгресс Организации Объединенных Наций По Предупреждению Преступности И Уголовному Правосудию. Семинар-Практикум 6: Меры По Борьбе Против Преступлений, Связанных С Использованием Компьютеров.' (Documents-dds-ny.un.org, 2022) <https://documents-dds-ny.un.org/doc/UNDOC/GEN/V05/822/61/PDF/V0582261.pdf?OpenElement> accessed 7 March 2022

[74] 'Конвенция О Компьютерных Преступлениях (Будапешт, 23 Ноября 2001 Года)' (*Rm.coe.int*, 2022) <https://rm.coe.int/1680081580> accessed 11 March 2022

3) в крупном размере;

4) лицом, уполномоченным на выполнение государственных функций, либо приравненным к нему лицом, либо должностным лицом, либо лицом, занимающим ответственную государственную должность, если оно сопряжено с использованием им своего служебного положения;

5) неоднократно;

6) в отношении двух или более лиц;

7) преступной группой;

8) в особо крупном размере.

Главное отличие составов «Мошенничество» и «Кибермошенничество» друг от друга заключаются в способе совершения. Применение электронно-вычислительных машин при совершении мошенничества дает общему составу данного преступления свою специфику, которые требуют, как специальных знаний, таки более сложного процесса расследования и доказывания сотрудниками правоохранительных органов, так как обман и злоупотребление доверием пользователя происходит на дистанции без фактического контакта с использованием технических возможностей. Урон, наносимый интернет мошенничества ими экономическим интересам государства и граждан, часто является существенным и не всегда восполним[75]. Это еще один аргумент в пользу выделения отдельного состава. Так как злоумышленник представляет общественную опасность путем большого охвата пользователей не только в рамках Республики Казахстан, а также за её пределами. Несмотря на то, что во многих государствах данный состав относится к главе «Компьютерных преступлений», в Уголовный кодекс Республики Казахстан необходимо ввести именно в главу 6 «Уголовные правонарушения против собственности». Это прежде всего обуславливается тем, что злоумышленники похищают собственность и право на собственность лица.

Если рассматривать состав преступления:

Объект – общественные отношения, направленные на охрану права собственности в киберпространстве.

Объективная сторона – хищение или приобретение права на него, путем обмана или злоупотребления доверием, а также ввода, изменения, удаления или блокирования компьютерных данных; или иного любого вмешательства в функционирование компьютерной системы с использованием информационных систем в целях приобретения материальной выгоды.

Субъект – вменяемое лицо, достигшее 16-летнего возраста. Субъектом квалифицированного мошенничества, совершаемого с использованием служебного положения (п. 2 ч. 2 и п. 2 ч. 3 ст. 190-1 УК РК), является лицо,

[75] Криминалистическая методика расследования отдельных видов преступлений: Учеб.: В 2 ч. / Под ред. А.П. Резвана, М.В. Субботиной. М., 2002. 88 с.

выполняющее управленческие функции в коммерческой или иной организации, либо должностное лицо.

Субъективная сторона – выражается в прямом умысле и корыстной целью. Преступник осознает, что путем обмана, злоупотреблением доверия, а также ввода, изменения, удаления или блокирования компьютерных данных и иным вмешательством совершает хищение. Мотивы совершения могут быть разными, например, В. Б. Вехов в таком большом разнообразии выделяет – корысть 66%[76]. Так как Интернет мошенничества основываются на знании стереотипного поведения человека, преследуя финансовую выгоду полученным преступным путем.

Помимо стереотипного поведения, злоумышленники оказывают влияние на психологическом уровне. В основном на такие уловки попадаются люди пожилого возраста. Например, в СКО к правоохранительным органам обратилась женщина шестидесяти лет, у которой мошенники, позвонив и представившись сотрудниками выманили 400 тысяч тенге, под предлогом того, что её «внук» попал в неприятную ситуацию[77]. Несмотря на наличие в органах внутренних дел Управления «К» и других подразделений при государственных органах, расследование компьютерных преступлений все ещё находятся в затруднительном состоянии.

В судебной практике Республике Казахстан используется понятие «Интернет мошенничество», однако выбор термина «Кибермошенничество» в предлагаемую статью исходит из того, что мошенничество осуществляется не только через Интернет, а совершается гораздо шире. Для того же ввода вредоносных ПО наличие Интернета не является обязательным фактором. Исходя из небольшой судебной практики, используемый термин не устоялся, а значит введение нового термина не составит большой проблемы.

3.2 Практические рекомендации по предотвращению преступлений мошенничества с применением информационных технологий.

Мир глобальной сети не стоит на месте, как и мошенники осуществляющие преступные деяния. С каждым днём изобретаются новые методы и способы совершения мошеннических действий в целях хищения чужого имущества, покушаясь на права человека. В большинстве случаев совершающие преступления – это люди, имеющие какие-либо познания в сфере информационных технологий. Несложно найти любую информацию во всемирной паутине и прокачать свои навыки для применения в

[76] Вехов В.Б. Компьютерные преступления: Способы совершения и раскрытия / Под ред. Б.П. Смагоринского. М.: Право и закон, 1996. С. 41.

[77] 'Телефонное Мошенничество На 400 Тысяч Тенге Расследуют Полицейские СКО' (*Gov.kz,* 2022) <https://www.gov.kz/memleket/entities/qriim/press/news/details/95459?lang=ru> accessed 16 May 2022

криминальной среде. Для этого методы борьбы и предотвращения должны быть на соответствующем уровне. Ответственность за сохранение порядка в киберпространстве должна лежать не только на плечах государства, но и на юридических и физических лицах в целях безопасности.

В рамках анализа текущей ситуации кибермошенничества, следует обратить внимание на следующие рекомендации:

1. Государственным органам и юридическим лицам, осуществляющим масштабную работу с персональными данными и безопасностью систем сбора и хранения таких данных (базами данных) необходимо:

a. Усилить контроль за безопасным использованием корпоративных локальных сетей и беспроводной связи: большую роль играют сами сотрудники компаний и государственных органов. Нужно обязать на сотрудников корпоративном уровне пройти курсы по информационной безопасности и ввести ответственность за несоблюдение и умалчивание фактов информационных угроз.

b. Усилить контроль по установке обязательных необходимых антивирусных программ, а также внедрить четкую систему отслеживания установки протоколов защиты на официальных сайтах организаций. Для этого ввести правовое регулирование и обозначить ответственность за нарушение или просрочку установки необходимых программ для сохранения безопасности.

2. На основе проведенного анализа и определения потенциальных причин кибермошенничества выявляется явная необходимость в организации систематических курсов повышения квалификации для сотрудников правоохранительных органов в сфере цифровой криминалистики.
3. Проводить профилактические мероприятия с населением, информируя о последствиях, кибергигиену и способах совершения кибермошенничества, повышая компьютерную и правовую грамотность. Объяснить важность сообщения правоохранительным органам о факте преступных деяний в глобальной сети.
4. В целях совместного и эффективного противодействия транснациональным преступным группам, которые специализирующимся на преступлениях в сфере информационных технологий, необходимо наладить международное сотрудничество для обмена опытом и оперативного реагирования на информационные угрозы.
5. Необходимо создать государственную структуру, которая объединит все заинтересованные органы и привлечет лучших специалистов из числа правоохранительных органов, IT специалистов, привлечет «хакеров» и экспертов в области кибербезопасности, которые обладают специальными знаниями и навыками. В последующем делиться

приобретёнными знаниями и взаимодействовать с государственными органами, финансовыми организациями и другими юридическими лицами.

6. Необходимо организовать курсы повышения квалификации для сотрудников правоохранительных органов, которые работают в области информационных технологий. Тем самым повысить качество работы с электронными доказательствами, проведения анализа, экспертиз и других оперативно-розыскных мероприятий. Помимо сотрудников правоохранительных органов также обязать пройти подготовку и повысить профессиональный уровень судей.

Данные практические рекомендации поспособствуют снижению не только кибермошенничества, но и киберпреступности в целом. Они были разработаны исходя из существующих проблем в правовом поле, практическом применении, а также на основании консультации с действующим экспертом в области кибербезопасности.

ЗАКЛЮЧЕНИЕ

Информационные технологии охватывают практически все сферы деятельности человека. Наряду с новыми возможностями, новая среда все чаще становится объектом для противоправных действий. В связи с глобальной цифровизацией борьба с преступностью в киберпространстве становится приоритетным направлением на международном уровне.

Развитие киберпреступности в отличии от других сфер деятельности происходить стремительно быстро. Распространение технологий в современном обществе меняет образ жизни людей[78]. Интернет-мошенничество не знает географических границ. Вне зависимости от того в какой вы стране, в каком часовом поясе и какой деятельностью занимаетесь – злоумышленник удаленно может получить доступ к вашим персональным данным преступным путем, что в дальнейшем может привести к большим финансовым потерям.

Динамика роста согласно статистическим данным и раскрываемость мошенничества в Интернете сигнализирует о проблемах в расследовании правоохранительными органами, необходимости усовершенствовании правовых механизмов и методов противодействия. Предпринимая меры по разработке рекомендаций, пособий и методик для мониторинга преступлений значительно повысит показатель раскрываемости. Нормотворчество и взгляд прогрессивных, компетентных специалистов в юриспруденции, финансах и в сфере IT технологий приблизят к быстрому и эффективному реагированию на инциденты.

Поставленные цели и задачи исследовательской работы были достигнуты: был проведен комплексный анализ доктрин, законодательств лучших зарубежных стран; были выявлены пробелы в действующем законодательстве, а также предложения по внесению изменений в Уголовный кодекс Республики Казахстан; изучены передовые практики по противодействию и расследованию кибермошенничества в зарубежных странах; разработаны рекомендации по совершенствованию инструментов и методов предотвращения цифрового мошенничества.

На основании того, что в исследовательских кругах вопросы о введении отдельного состава такого вида преступления, как мошенничество с использованием инфокоммуникационных технологий остаются актуальными и дискуссионными, считаю, что в соответствии с изучением международного опыта передовых компьютерализованных государств необходимо ввести состав «Кибермошенничество» в действующий Уголовный кодекс Республики Казахстан, также есть необходимость ввести соответствующий термин и обобщить различные интерпретации данного

[78] Holt T, Bossler A, and Seigfried-Spellar K, *Cybercrime And Digital Forensics* (2nd edn, October 19, 2017 by Routledge, 743 p.)

феномена. Помимо улучшения нормативно-правовой базы, также стоит обратить особое внимание на улучшение кадровых служб для эффективной работы по предотвращению такого вида преступлений.

В странах, где пониженная координация информационных сетей может использоваться как транзитные каналы для осуществления преступных деяний в цифровом пространстве. В особенности, это касается тех государств, у которых отсутствует правовая ответственность за совершение преступлений, в том числе за самый распространённый из них – мошенничество. Наличие жестких санкций изначально препятствуют на подсознательном уровне совершать неправомерные деяния. Вместе с правовыми основами нужно в совокупности охватывать и техническую составляющую. Системы могут быть уязвимыми до тех пор, пока стандарты безопасности не будут внедряться во все структуры, в особенности там, где храниться большая база персональных данных.

Комплексное рассмотрение данной проблемы как со стороны юриспруденции, цифровой криминалистики и сферы IT поможет эффективному раскрытию и предотвращению кибермошенничества. Развитие и модернизация законодательства требует тщательного анализа, и напрямую зависит от алгоритма действий и рекомендаций со стороны сотрудников правоохранительных органов, которые обладают специальными знаниями.

БИБЛИОГРАФИЯ

Книги:

- Волженкин Б. В. Мошенничество: Серия «Современные стандарты в уголовном праве и уголовном процессе». СПб., 1998. 36 с. (21 с.)
- Вехов В.Б. Компьютерные преступления: Способы совершения и раскрытия / Под ред. Б.П. Смагоринского. М.: Право и закон, 1996. С. 41.
- Комаров А.А. Криминологическая экспертиза некоторых законопроектов, связанных с Интернетом //Современное право. - 2009. - №6. - С. 109-113.
- Криминалистическая методика расследования отдельных видов преступлений: Учеб.: В 2 ч. / Под ред. А.П. Резвана, М.В. Субботиной. М., 2002. 88 с.
- Holt T, Bossler A, and Seigfried-Spellar K, Cybercrime And Digital Forensics (2nd edn, October 19, 2017 by Routledge, 743 p.)
- Button M, Hock B, and Shepherd D, Economic Crime From Conception to Response (1st edn, Published April 25, 2022 by Routledge, 314 p.)

Статьи:

- Красовская Наталия Рудольфовна, Гуляев Андрей Анатольевич 'К ВОПРОСУ О КИБЕРМОШЕННИЧЕСТВЕ' (КиберЛенинка, 2022) <https://cyberleninka.ru/article/n/k-voprosu-o-kibermoshennichestve>
- Погорелова М. А., 'Правовое Регулирование Распространения Информации В Сети Интернет В Условиях Глобализации' (*Cyberleninka.ru*, 2022) <https://cyberleninka.ru/article/n/pravovoe-regulirovanie-rasprostraneniya-informatsii-v-seti-internet-v-usloviyah-globalizatsii/viewer>
- Antipov A, 'Лучшие Методы Предотвращения Атак Компрометации Деловой Электронной Почты (BEC)' (Securitylab.ru, 2022) <https://www.securitylab.ru/blog/personal/bezmaly/351180.php>
- Николайчук А, 'Обзор Законодательства Молдовы: Борьба С Киберпреступностью' (Digital Report, 2022) <https://digital.report/zakonodatelstvo-moldovy-infobezopasnost-9/>
- Тихонравов Е, 'Принцип Nullum Crimen Sine Lege В Истории Отечественного Уголовного Права' (Cyberleninka.ru, 2022) <https://cyberleninka.ru/article/n/printsip-nullum-crimen-sine-lege-v-istorii-otechestvennogo-ugolovnogo-prava/viewer>
- 'FRAUD IN THE INTERNET: CRIMINOLOGICAL CHARACTERISTICS AND QUALIFICATION PROBLEMS' (Cyberleninka.ru, 2022) <https://cyberleninka.ru/article/n/moshennichestvo-v-seti-internet-kriminologicheskaya-harakteristika-i-problemy-kvalifikatsii/viewer>

- Л.С. Хафизова, 'Система Правового Противодействия Финансовому Мошенничеству В России В Современных Условиях' (КиберЛенинка, 2022) <https://cyberleninka.ru/article/n/sistema-pravovogo-protivodeystviya-finansovomu-moshennichestvu-v-rossii-v-sovremennyh-usloviyah>

Нормативно правовые акты:

- 'Уголовный Кодекс Республики Казахстан - ИПС "Әділет"' (Adilet.zan.kz, 2022) <https://adilet.zan.kz/rus/docs/K1400000226>
- 'Комментарий К Уголовному Кодексу Республики Казахстан (Особенная Часть)' (Zakon.uchet.kz, 2022) <https://zakon.uchet.kz/rus/docs/T9700167_1_> accessed 2 May 2022
- Об утверждении Концепции кибербезопасности ("Киберщит Казахстана") Постановление Правительства Республики Казахстан от 30 июня 2017 года № 407 https://adilet.zan.kz/rus/docs/P1700000407
- "Уголовный Кодекс Российской Федерации" (УК РФ) От 13.06.1996 N 63-ФЗ (Последняя Редакция) \ Консультантплюс' (Consultant.ru, 2022) <http://www.consultant.ru/document/cons_doc_LAW_10699/>
- '18 U.S. Code § 1343 - Fraud By Wire, Radio, Or Television' (LII / Legal Information Institute, 2022) <https://www.law.cornell.edu/uscode/text/18/1343>
- 'Chapter 952 - Penal Code: Offenses' (Cga.ct.gov, 2022) <https://www.cga.ct.gov/current/pub/chap_952.htm#sec_53a-125c>
- 'Michigan Computer Laws § 750.409B' (Casetext.com, 2022) <https://casetext.com/statute/michigan-compiled-laws/chapter-750-michigan-penal-code/subchapter-miscellaneous/section-750409b-ransomware-possession-use-prohibition-violation-as-felony-penalty-ransomware-defined>
- 'North Dakota Century Code T54c59.1' (Ndlegis.gov, 2022) <https://ndlegis.gov/cencode/t54c59-1.pdf#nameddest=54-59p1-06>
- 'Criminal Law Of The People's Republic Of China' (Cybercrimelaw.net, 2022) <https://www.cybercrimelaw.net/China.html>
- УК РФ Статья 159.6. Мошенничество В Сфере Компьютерной Информации \ Консультантплюс (Consultant.ru, 2022) <http://www.consultant.ru/document/cons_doc_LAW_10699/51c53d82b60ac8c009745bdea3838d507064c6d3/>
- 'ЗАКОН Республики Молдовы № 20 От 03.02.2009 По Предотвращению И Борьбе С Киберпреступностью' (Legis.md, 2022) <https://www.legis.md/cautare/getResults?doc_id=12742&lang=ro>

- 'Уголовный Кодекс Республики Молдовы' (Legislationline.org, 2022) <https://www.legislationline.org/download/id/10026/file/MOLD_CC_2021_ru.pdf>
- 'German Criminal Code (Criminal Code In The Version Published On 13 November 1998 (Federal Law Gazette I, P. 3322), As Last Amended By Article 2 Of The Act Of 19 June 2019 (Federal Law Gazette I, P. 844))' (Legislationline.org, 2022) <https://www.legislationline.org/download/id/10003/file/GERM_CC_en.pdf>
- 'Уголовный Кодекс Эстонии' (Legislationline.org, 2022) <https://www.legislationline.org/download/id/6462/file/Estonia_CCвнутр_as_of_2002_ru.pdf>
- 'Конвенция О Компьютерных Преступлениях (Будапешт, 23 Ноября 2001 Года)' (Rm.coe.int, 2022) <https://rm.coe.int/1680081580>

Интернет ресурсы:

- 'Киберпреступность (Будапештская Конвенция)' (Воздействие Европейской конвенции о правах человека, 2022) <https://www.coe.int/ru/web/impact-convention-human-rights/convention-on-cybercrime#/Sweden>
- 'INTERPOL Launches Centre Against Financial Crime And Corruption' (Interpol.int, 2022) <https://www.interpol.int/News-and-Events/News/2022/INTERPOL-launches-centre-against-financial-crime-and-corruption>
- 'Одиннадцатый Конгресс Организации Объединенных Наций По Предупреждению Преступности И Уголовному Правосудию' (Documents-dds-ny.un.org, 2022) <https://documents-dds-ny.un.org/doc/UNDOC/GEN/V05/822/61/PDF/V0582261.pdf?OpenElement>
- 'Опыт Цифровизации МВД Казахстана Вызвал Интерес У Зарубежных Экспертов' (polisia.kz, 2022) <https://polisia.kz/ru/opyt-tsifrovizatsii-mvd-kazahstana-vyzval-interes-u-zarubezhnyh-ekspertov/>
- 'ЗЛОУПОТРЕБЛЕНИЕ Толковый Словарь Ожегова Онлайн' (Slovarozhegova.ru, 2022) <https://slovarozhegova.ru/word.php?wordid=9249>
- 'Cyberfraud' (Dictionary.cambridge.org, 2022) <https://dictionary.cambridge.org/ru/%D1%81%D0%BB%D0%BE%D0%B2%D0%B0%D1%80%D1%8C/%D0%B0%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9/cyberfraud>

- 'What Is Cyber Fraud? - Deltanet' (DeltaNet, 2022) <https://www.delta-net.com/knowledge-base/compliance/fraud-awareness/what-is-cyber-fraud/>
- 'Что Такое “Фишинг”' (Encyclopedia.kaspersky.ru, 2022) <https://encyclopedia.kaspersky.ru/knowledge/what-is-phishing/>
- 'Фишинг, Вишинг, Смишинг, Фарминг — В Чем Разница' (Protectimus.com, 2022) <https://www.protectimus.com/blog/ru-phishing-vishing-smishing-pharming/>
- 'Welcome To FBI.Gov | Federal Bureau Of Investigation' (Federal Bureau of Investigation, 2022) <https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/nigerian-letter-or-419-fraud>
- 'Названы Распространенные Схемы Кибермошенничества' (Деловой портал Капитал.кз, 2022) <https://kapital.kz/gosudarstvo/100440/nazvany-rasprostranennyye-skhemy-kibermoshennichestva.html>
- Inbusiness.kz. 2022. Раскрываемость киберпреступлений в Казахстане не превышает 3%. [online] Available at: <https://inbusiness.kz/ru/news/raskryvaemost-kiberprestuplenij-v-kazahstane-ne-prevyshaet-3> .
- Studbooks. 2022. Использование специальных познаний при расследовании мошенничества в сфере компьютерной информации. [online] Available at: <https://studbooks.net/2427202/pravo/ispolzovanie_spetsialnyh_poznaniy_rassledovanii_moshennichestva_sfere_kompyuternoy_informatsii>.
- profit.kz. 2022. Интернет-мошенничество в Казахстане: тысячи таких дел остаются не раскрытыми. [online] Available at: <https://profit.kz/news/58861/Internet-moshennichestvo-v-Kazahstane-tisyachi-takih-del-ostautsya-ne-raskritimi/>
- Dslib.net. 2022. Расследование мошенничества в сфере компьютерной информации: научно-теоретическая основа и прикладные аспекты первоначального этапа. [online] Available at: <http://www.dslib.net/finans-pravo/rassledovanie-moshennichestva-v-sfere-kompjuternoj-informacii-nauchno-teoreticheskaja.html>
- 'Ущерб От Деятельности Интернет-Мошенников В США Достиг Рекордных $6,9 Млрд — ФБР | Digital Russia' (Digital Russia, 2022) <https://d-russia.ru/ushherb-ot-dejatelnosti-internet-moshennikov-v-ssha-dostig-rekordnyh-6-9-mlrd-fbr.html>
- 'Internet Crime Report 2021' (Ic3.gov, 2022) <https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf>
- 'Statutes & Constitution :View Statutes : Online Sunshine' (Leg.state.fl.us, 2022)

<http://www.leg.state.fl.us/STATUTES/index.cfm?App_mode=Display_Statute&Search_String=&URL=0600-0699/0668/Sections/0668.703.html>

- 'Reporting And Policing Internet Crimes In China' (Hg.org, 2022) <https://www.hg.org/legal-articles/reporting-and-policing-internet-crimes-in-china-22958>
- 'Cybercrime In China' (Unodc.org, 2022) <https://www.unodc.org/documents/Cybercrime/English.pdf>
- 'О Национальной Платежной Системе От 27 Июня 2011 - Docs.Cntd.Ru' (Docs.cntd.ru, 2022) <https://docs.cntd.ru/document/902286143>
- 'Эксперты Назвали Самый Популярный Способ Мошенничества В Интернете' (rbc.ru, 2022) <https://www.rbc.ru/technology_and_media/09/02/2021/602184e19a794726a2165b6b>
- 'Почему Киберпреступления – Угроза Национальной Безопасности' (Ведомости, 2022) <https://www.vedomosti.ru/technology/articles/2021/12/07/899278-kiberprestupleniya-bezopasnosti>
- 'Каждый Десятый Россиянин Сталкивался С Продавцами-Мошенниками В Интернете — НАФИ' (Nafi.ru, 2022) <https://nafi.ru/analytics/kazhdyy-desyatyy-rossiyanin-stalkivalsya-s-prodavtsami-moshennikami-v-internete/>
- 'Каждый Десятый Россиянин Сталкивался С Продавцами-Мошенниками В Интернете — НАФИ' (Nafi.ru, 2022) <https://nafi.ru/analytics/kazhdyy-desyatyy-rossiyanin-stalkivalsya-s-prodavtsami-moshennikami-v-internete/>
- 'Почему Киберпреступления – Угроза Национальной Безопасности' (Ведомости, 2022) <https://www.vedomosti.ru/technology/articles/2021/12/07/899278-kiberprestupleniya-bezopasnosti>
- 'Преступления Против Собственности : Уголовный Кодекс Украины : Уголовный Кодекс : Кодексы Украины : Недвижимость Украины - Meget.Kiev.Ua' (2022) <https://meget.kiev.ua/kodeks/ugolovniy-kodeks/razdel-1-6/>
- 'В Прошлом Году В Украине Активизировались Интернет-Мошенники. В НБУ Рассказали, По Каким Схемам Они Работают | Громадское Телевидение' (Hromadske.ua, 2022) <https://hromadske.ua/ru/posts/v-proshlom-godu-v-ukraine-aktivizirovalis-internet-moshenniki-v-nbu-rasskazali-po-kakim-shemam-oni-rabotayut>

- 'Мошенники Выманивают Деньги В Украинцев Под Видом Помощи Переселенцам - Полиция' (Ukrinform.ru, 2022) <https://www.ukrinform.ru/rubric-society/3462308-mosenniki-vymanivaut-dengi-u-ukraincev-pod-vidom-pomosi-pereselencam-policia.html>
- 'Киберполиция Рассказала Об Основных Мошеннических «Схемах» В Условиях Военного Положения' (Ukrinform.ru, 2022) <https://www.ukrinform.ru/rubric-society/3449782-kiberpolicia-rasskazala-ob-osnovnyh-mosenniceskih-shemah-v-usloviah-voennogo-polozenia.html>
- 'МВД: Киберполиция Украины Переходит На Новый Уровень Работы И Объявляет Большой Набор Специалистов - ITC.Ua' (ITC.ua, 2022) <https://itc.ua/news/mvd-kiberpolicziya-ukrainy-perehodit-na-novyj-uroven-raboty-i-obyavlyaet-bolshoj-nabor-speczialistov/>
- 'IT & Cyber-Sicherheit' (Bundesministerium des Innern und für Heimat, 2022) <https://www.bmi.bund.de/DE/themen/it-und-digitalpolitik/it-und-cybersicherheit/it-und-cybersicherheit-node.html;jsessionid=B5FDE9BF4B544D519A20DBC7860E9E12.1_cid364>
- 'Expert International Cybercrime Taskforce Is Launched To Tackle Online Crime | Europol' (Europol, 2022) <https://www.europol.europa.eu/media-press/newsroom/news/expert-international-cybercrime-taskforce-launched-to-tackle-online-crime-0>
- 'Cybercrime Policies/Strategies In Germany' (Octopus Cybercrime Community, 2022) <https://www.coe.int/en/web/octopus/country-wiki-ap//asset_publisher/CmDb7M4RGb4Z/content/germany/pop_up?_101_INSTANCE_CmDb7M4RGb4Z_viewMode=print&_101_INSTANCE_CmDb7M4RGb4Z_languageId=en_GB>
- 'Веб-Констебли' (Juristaitab.ee, 2022) <https://www.juristaitab.ee/ru/chabo/veb-konstebli>
- 'Самые Популярные Виды Мошенничества В Эстонии И Как Государство Задерживает Иностранных Киберпреступников' (www.gloss.ee, 2022) <https://www.gloss.ee/2020/11/11/samye-populyarnye-vidy-moshennichestva-v-estonii-i-kak-gosudarstvo-zaderzhivaet-inostrannyh-kiberprestupnikov/>
- 'Кибермошенники Стали Использовать Данные Из Регистра Госзакупок' (ERR, 2022) <https://rus.err.ee/1120167/kibermoshenniki-stali-ispolzovat-dannye-iz-registra-goszakupok>
- 'Опасный Tinder И "Любовные Мошенничества": Какими Способами В 2021 Году У Жителей Эстонии Выманили 10 Млн

Евро?' (Delfi RUS, 2022) <https://rus.delfi.ee/statja/95621501/opasnyy-tinder-i-lyubovnye-moshennichestva-kakimi-sposobami-v-2021-godu-u-zhiteley-estonii-vymanili-10-mln-evro>

- 'Профилактика И Рекомендации | Riigi Infosüsteemi Amet' (Ria.ee, 2022) <https://www.ria.ee/ru/kiberbezopasnost/profilaktika-i-rekomendacii.html>
- 'Полиция Эстонской Республики' (Eurasialaw.ru, 2022) <https://eurasialaw.ru/nashi-rubriki/politsiya-gosudarstv-mira/politsiya-estonskoj-respubliki>
- 'Мошенники Коронавирусного Времени — Что Следует Знать И Как Защититься' (Tribuna.ee, 2022) <https://tribuna.ee/tribuna/crime/novye-vidy-moshennichestva-estonia/>
- 'Вдвое Выросло Количество Интернет-Мошенничеств В Казахстане' (profit.kz, 2022) <https://profit.kz/news/62084/Vdvoe-viroslo-kolichestvo-internet-moshennichestv-v-Kazahstane/>
- 'A Comparative Study Of Cybercrime In Criminal Law: China, US, England, Singapore And The Council Of Europe' (Repub.eur.nl, 2022) <https://repub.eur.nl/pub/94604/PROOF-Qianyun-Wang-BW-1-.pdf>
- A/CONF.203/14 O, 'Одиннадцатый Конгресс Организации Объединенных Наций По Предупреждению Преступности И Уголовному Правосудию. Семинар-Практикум 6: Меры По Борьбе Против Преступлений, Связанных С Использованием Компьютеров.' (Documents-dds-ny.un.org, 2022) <https://documents-dds-ny.un.org/doc/UNDOC/GEN/V05/822/61/PDF/V0582261.pdf?OpenElement>
- 'Телефонное Мошенничество На 400 Тысяч Тенге Расследуют Полицейские СКО' (Gov.kz, 2022) <https://www.gov.kz/memleket/entities/qriim/press/news/details/95459?lang=ru>