Оригинальная статья / Original article

УДК 343.71

https://doi.org/10.21869/2223-1501-2023-13-6-199-208

О способах совершения преступлений против собственности в сети Интернет

А. В. Москальков[1] ✉

[1]Московский университет имени А.С. Грибоедова
ул. Новая Басманная, д. 35/1, г. Москва 105066, Российская Федерация

✉ e-mail: 11amo@list.ru

Резюме

Актуальность *статьи обусловлена стремительным ростом в России корыстных преступлений, совершаемых с использованием информационно-телекоммуникационных технологий. Наибольшая доля таких преступлений в структуре преступных посягательств на собственность приходится на мошенничество и вымогательство. В статье приводится оригинальный анализ способов их совершения, получивших наибольшее распространение в Глобальной сети. Делается прогноз о том, что данный вид киберпреступности в будущем может стать одной из серьезных проблем, поскольку преступные схемы использования сетевых интернет-ресурсов постоянно обновляются, а установить все способы не представляется возможным.*

Цель *исследования состоит в дополнении научного знания об имеющихся и новых способах совершения корыстных преступлений с использованием сети Интернет для эффективного противодействия им.*

Задачи*: на основе судебной практики, сообщений средств массовой информации, интернет-источников выявить имеющиеся и новые способы совершения корыстных преступлений в сети Интернет.*

Методология. *При написании работы применялись методы научного познания (анализ, синтез, индукция и дедукция), а также статистический, документальный и формально-логический методы.*

Результаты исследования *состоят в описании имеющихся и установлении новых способов совершения преступлений против собственности, влияющих на качественные и количественные показатели корыстной преступности в целом. Восполнен определенный пробел криминологической науки по проблемам хищения чужого имущества путем мошеннических действий и вымогательства в сети Интернет. Полученные результаты могут быть использованы в практической деятельности правоохранительных органов.*

Вывод. *Социально опасные последствия совершения киберпреступлений против собственности определяются их массовостью, огромным числом потерпевших, большим ущербом и высокой латентностью. Стремительная виртуализация всех сфер жизни общества позволяет прогнозировать последовательное увеличение посягательств против собственности в сети Интернет.*

Ключевые слова*: преступления против собственности; мошенничество; вымогательство; интернет; информационные технологии.*

Конфликт интересов*: Автор декларирует отсутствие явных и потенциальных конфликтов интересов, связанных с публикацией настоящей статьи.*

Для цитирования: Москальков А. В. О способах совершения преступлений против собственности в сети Интернет // Известия Юго-Западного государственного университета. Серия: История и право. 2023. Т. 13, № 6. С. 199–208. https://doi.org/10.21869/2223-1501-2023-13-6-199-208.

Поступила в редакцию 20.10.2023 Принята к публикации 24.11.2023 Опубликована 25.12.2023

About Ways to Commit Crimes Against Property on the Internet

Artem V. Moskalkov[1] ✉

[1]Moscow University A. S. Griboedov
35/1 Novaya Basmannaya Str., Moscow 105066, Russian Federation

✉ e-mail: 11amo@list.ru

Abstract

Relevance *of the article is due to the rapid growth in Russia of mercenary crimes committed using information and telecommunication technologies. The largest share of such crimes in the structure of criminal encroachments on property falls on fraud and extortion. The article provides an original analysis of the methods of their commission, which have become most widespread on the Global Network. It is predicted that this type of cybercrime in the future may become one of the serious problems, since criminal schemes for using network Internet resources are constantly updated, and it is not possible to establish all methods.*

The purpose *of the study is to supplement scientific knowledge of available and new ways of committing mercenary crimes using the Internet to effectively counter them.*

Objectives: *on the basis of judicial practice, media reports, Internet sources, to identify existing and new methods of committing mercenary crimes on the Internet.*

Methodology*. When writing the work, methods of scientific knowledge (analysis, synthesis, induction and deduction), as well as statistical, documentary and formal-logical methods were used.*

The results *of the study consist in describing the available and establishing new methods of committing crimes against property, affecting the qualitative and quantitative indicators of mercenary crime in general. A certain gap in criminological science on the problems of theft of someone else's property through fraudulent actions and extortion on the Internet has been filled. The results obtained can be used in the practical activities of law enforcement agencies.*

Conclusion. *The socially dangerous consequences of committing cybercrimes against property are determined by their mass, huge number of victims, great damage and high latency. Rapid virtualization of all areas of society makes it possible to predict a consistent increase in encroachments against property on the Internet.*

Keywords*: crimes against property; fraud; extortion; Internet; information technology.*

Conflict of interest: *The Author declare the absence of obvious and potential conflicts of interest related to the publication of this article.*

For citation: Moskalkov A. V. About Ways to Commit Crimes Against Property on the Internet. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Seriya: Istoriya i pravo = Proceedings of the Southwest State University. Series: History and Law*. 2023; 13(6): 199–208. (In Russ.) https://doi.org/10.21869/2223-1501-2023-13-6-199-208

Received 20.10.2023 Accepted 24.11.2023 Published 25.12.2023

***

Введение

В условиях стремительной модификации Глобальная сеть превратилась в площадку для криминальной деятельности. По подсчетам экспертов, на долю преступлений, совершаемых с использованием сети Интернет, приходится одна треть от всех регистрируемых ежегодно преступлений в России (26,6%) [1, с. 218]. Трансграничность, анонимность, отсутствие цифровых следов и невозможность закрепить многие доказательства криминальной деятельности на материальном носителе – все это многократно увеличивает риски совершения преступлений, и в том числе против собственности. Интернет-ресурсы (социальные сети, сайты знакомств, иные платформы) с открытыми персональными данными пользователей используются в качестве инструмента для мошенничества, вымогательства и краж. По данным МВД РФ, количество преступлений против собственности с применением информационных технологий в 2022 г. в России составило: по ст.

158 УК РФ «Кража» – 113565; по ст. 159 УК РФ «Мошенничество» – 249984; по ст. 159[3] УК РФ «Мошенничество с использованием электронных средств платежа» – 7288; по ст. 159[6] УК РФ «Мошенничество в сфере компьютерной информации» – 334; по ст. 163 УК РФ «Вымогательство» – 5721[1]. Наблюдается рост количества киберпреступлений против собственности, которые совершают ранее судимые лица. Очевидно, эта статистика не отражает действительного масштаба преступности, поскольку жертвы не всегда обращаются в правоохранительные органы, а виновные избегают уголовного преследования. Другими словами, фактические данные динамики и уровня преступлений, совершаемых против собственности с использованием цифровых технологий, во много раз превышают показатели, зарегистрированные официальной уголовной статистикой. На проблему защиты прав жертв дистанционных хищений обращено на самом высоком государственном уровне. Президент Российской Федерации по итогам заседания Совета по развитию гражданского общества и правам человека дал поручение Правительству РФ и Банку РФ разработать механизм выплаты кредитными организациями денежной компенсации клиентам, у которых мошенниками были похищены деньги[2].

Учитывая общественную опасность преступлений в сети Интернет, специалисты по уголовному праву и криминологии приступили к основательному анализу трендов киберпреступности против собственности. Исследованию вопросов, связанных с корыстной интернет-преступностью, посвящены труды многих ученых [2, с. 44; 3, с. 126; 4, с. 72]. Вместе с тем особую актуальность имеют исследования, связанные с изучением способов совершения таких преступлений по причине их постоянной модернизации.

Методология

При написании научной статьи совокупность общенаучных и частнонаучных методов исследования определялась ее темой. Методы анализа и синтеза, индукции и дедукции применялись для формулирования поисковых запросов, выявления и описания имеющихся и новых способов совершения преступлений против собственности в сети Интернет и формулирования прогнозов дальнейшего развития корыстной киберпреступности. Для обоснования актуальности проблемы исследования, изучения научных трудов по рассматриваемой тематике, данных уголовной статистики и приговоров судов, интернет-источников, содержащих описание способов виртуальных хищений, применялись статистический и документальный методы. Описать полученные результаты, систематизировать материал и сформулировать выводы исследования позволил формально-логический метод.

Результаты и их обсуждение

Для осуществления анализа способов совершения преступлений против собственности в сети Интернет необходимо выделить конкретные деяния (составы), образующие эту группу. В отечественной науке теоретики предлагают разные варианты группирования преступлений против собственности, совершаемых с использованием информационных технологий: и по объекту преступлений (собственность), и по способу их совершения (с использованием сети Интернет). Учитывая представленные в теории позиции правоведов, следует согласиться в том, что к таким составам преступлений относятся: кража с банковского счета, а равно совершенная в отношении электронных

[1] Состояние преступности за январь-декабрь 2022 года // Министерство внутренних дел Рос. Федерации: сайт. URL: https://мвд.рф/reports/item/35396677/?ysclid=lofyqpnkjp374098658 (дата обращения: 22.09.2023).

[2] Перечень поручений по итогам заседания Совета по развитию гражданского общества и правам человека // Президент России: офиц. сайт. URL: http://www.kremlin.ru/acts/assignments/ orders/70349 (дата обращения: 17.09.2023).

денежных средств (п. «г» ч. 3 ст. 158 УК РФ); мошенничество (ст. 159 УК РФ); мошенничество в сфере кредитования (ст. 159^1 УК РФ); мошенничество с использованием электронных средств платежа (ст. 159^3 УК РФ); мошенничество в сфере компьютерной информации (ст. 159^6 УКРФ); присвоение и растрата (ст. 160 УК РФ); вымогательство (ст. 163 УК РФ); причинение имущественного ущерба путём обмана и злоупотребления доверием (ст. 165 УК РФ); умышленное уничтожение или повреждение чужого имущества (ст. 167 УК РФ) [5, с. 30].

Правоприменительная практика показывает, что наиболее распространёнными преступлениями против собственности, совершаемыми с использованием информационных технологий, являются мошенничество и вымогательство.

1. *Мошенничество.* При анализе способов мошенничества с использованием информационных технологий исследователи отмечают их разнообразие и общий алгоритм действий [6, с. 64]. При этом верно подмечается, что в статистических показателях только три состава мошенничества находят отражение (ст. 159, 159^3, 159^6 УК РФ), что не отражает действительной картины корыстной преступности [7, с. 98]. Значительную долю мошеннических действий составляет так называемое «инфоцыганство». Его показатели значительно возросли в период пандемии COVID-19 [8, с. 180]. Оно процветает на просторах Интернета, в социальных сетях, в том числе запрещенных в России, что позволяет вовлечь многомиллионную аудиторию в массовую покупку курсов, обучений, услуг, товаров и др. [9, с. 172] Примерами мошенничества в онлайн-сфере являются всевозможные обучения у псевдо-онлайн-коучей, оказание экстрасенсорных, психологических, астрологических услуг, псевдолечение или целительство, цыганские предсказания и др. (*мошенничество в сфере услуг*).

Мошенники заманивают жертву бесплатными курсами, мероприятиями, обещая дать базовые знания «чтобы быть успешным», входят в доверие, а после начинается «раскрутка» на деньги. Примерами тому служат различные марафоны инфоцыган в соцсетях («Марафон желаний» Е. Блиновской, «Денежный марафон» В. Чекалиной, «Я выбираю тебя» Н. Серовской, «Стратегии на миллион» О. Самойловой, «Мышление миллионера» Г. Гасанова и др.) [10, с. 169]. Опасность инфоцыганства как явления с высоким криминогенным потенциалом состоит в том, что блогеры продают не качественный онлайн-продукт, помогающий выработать профессиональные навыки, а манипулируют массовым сознанием, вселяют уверенность в достижении целей за короткий срок без каких-либо знаний и усилий. Как справедливо отмечает член Совета по правам человека при Президенте РФ И. С. Ашманов, инфоцыгане сначала «создают образ депрессивности, скуки и нищеты», убеждают «в необходимости реализовывать мечты», а затем дают весьма банальные советы, например, «полюбить себя», научиться «быть в ресурсном состоянии»[1]. К сожалению, правоохранители не выработали методику противодействия этому виду мошенничества [11, с. 28]. «Инфоцыгане» либо уходят от какого-либо наказания, либо привлекаются к уголовной ответственности за совершение не мошенничества, а других преступлений[2].

Освоив компьютерные технологии, злоумышленники подделывают сайты благотворительных фондов, интернет-магазинов, банков, государственных учреждений [12, с. 81]. Так, мошенники в одной из социальных сетей размещали

[1] Госдума готовится дать бой инфоцыганам // Царьград: сайт. URL: https:// tsargrad.tv/news/gosduma-gotovitsja-dat-boj-infocyganam_497311 (дата обращения: 22.09.2023).

[2] «У следователей несколько вариантов». Что ждет Елену Блиновскую // РИА Новости. 2023. 27 апр. URL: https://ria.ru/20230427/blinovskaya-1868236065.html?ysclid=loely78vzu793601178 (дата обращения: 22.09.2023).

объявления о продаже вещей известных брендов с большой скидкой. Заказ оплачивался сразу, а затем потерпевшие получали по почте дешевые тряпки. Вернуть деньги было невозможно, т. к. телефоны продавцов были заблокированы. Судя по количеству посылок, отправленных в разные регионы страны, число потерпевших может составить больше тысячи человек[1].

Мошенниками создаются и сайты с объявлениями об оказании тех или иных услуг, в том числе запрещенных (написание дипломных работ, диссертаций, оккультные, психологические, связанные с нетрадиционным лечением и др.). К примеру, на сайтах об оказании сексуальных услуг для завлечения клиентов размещается галерея фотографий красивых девушек, якобы занимающихся проституцией. Клиент переводит предоплату за будущую услугу, а после требований о возврате денег мошенники блокируют его доступ к сайту или странице в Сети, шантажируют «заказом» или угрожают физической расправой[2]. Преступники уверены, что обманутая жертва не обратится в правоохранительные органы, поскольку устыдится своего грехопадения. К этому виду массового обмана можно отнести и букмекерские конторы в Интернете, когда осуществляется продажа «беспроигрышных» стратегий, гарантирующих выигрыш (он подтверждается подделкой скриншотов, чеками банкоматов), а поток потенциальных жертв (воронка) генерируется сайтами, соцсетями и мессенджерами [13, с. 40].

Отдельным случаем является такая разновидность мошенничества, как романтическое («на почве любви»). Так, жительница г. Москвы познакомилась в Интернете с иностранцем по имени Дэвид Леонардо. В ходе переписки кавалер изъявил желание приехать в свой отпуск для личного знакомства. Чтобы получить отпускные, Леонардо нужно было заплатить за них компании 350 тыс. рублей. Он попросил их у женщины, которая и перевела данную сумму «компании». Позже на почту женщине пришло новое письмо от «компании», в которой работал иностранец, что необходимо еще 350 тыс. руб. После перевода указанной суммы женщина рассказала эту историю подруге. Она нашла «Дэвида» под другими именами на сайтах знакомств[3]. А как действуют виртуальные «мошенницы на доверии» в отношении мужчин? Они заводят аккаунты в соцсетях и начинают активно комментировать фото, ставить «лайки», а затем вступают в легкую переписку с будущей жертвой. Новая знакомая может быть даже замужем и с детьми, хорошо образована и рассуждает о политике, экономике, искусстве, фильмах, домашнем уюте, люксовой одежде и дорогих курортах. Затем сетевая красотка добавляет драмы (развод с мужем, болезнь, потеря работы и т. д.) и просит перевести деньги на свой счет[4].

Еще одним примером мошенничества в сети Интернет является фродинг, при котором осуществляется несанкционированное списание денежных средств с банковской карты пользователя [14, с. 137]. Для хищения денежных средств у подписчиков злоумышленники также используют взломанный аккаунт с личными

[1] Задержаны аферисты, создавшие липовые сайты продаж // Российская газета. 2023. 19 марта. URL: https://rg.ru/2023/03/19/triapki-v-posylkah.html?ysclid=loen7r6o3n953655910 (дата обращения: 22.09.2023).

[2] Мошенники начали прикидываться в сети проститутками // Московский комсомолец. 2021. 20 февр. URL: https://www.mk.ru/ incident/2021/02/20/moshenniki-nachali-prikidy (дата обращения: 22.09.2023).

[3] Осторожно, мошенники! // Генеральная прокуратура Рос. Федерации: сайт. URL: https://epp.genproc.gov.ru/web/proc_77/activity/legal-education/fraud?item=91054747 (дата обращения: 25.10.2023).

[4] Как проститутки разводят мужчин в соцсетях // Московский комсомолец. 2014. 25 июля. URL: https://www.mk.ru/social/2014/07/25/kak-prostitutki-razvodyat-muzhchin-v-socsetyakh.html?ysclid=loele4oq2x864618296 (дата обращения: 22.09.2023).

данными пользователя (мошенничество под чужим именем) [15, с. 101]. Им рассылается сообщение от имени владельца страницы об экстренной ситуации с просьбой о переводе денежных средств. Чтобы расположить жертву, вызвать доверие (социальная инженерия), мошенники покупают базы персональных данных, которые «утекли» в теневой сегмент Интернета и выставлены на продажу[1].

По наблюдению криминологов, в последние годы фиксируется изменение в мотивации IT-преступников, которыми меньше совершается неправомерный доступ к закрытой информации, а все больше наносится репутационный ущерб бизнесу. Из недавних примеров масштабной компрометации личных данных клиентов утечка у таких гигантов, как Сбер, Яндекс-еда, «Билайн», ВТБ, РЖД, авиакомпания «Победа» и др.[2] По мнению М. А. Простосердова, «кибермошенничество можно рассматривать как следующую ступень развития таких преступлений, как неправомерный доступ к компьютерной информации (ст. 272 УК РФ) и создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ)» [16, с. 151].

2. *Вымогательство* (ст. 163 УК РФ). Представители правоохранительных органов отмечают рост случаев дистанционного вымогательства, связанного с угрозой распространения позорящих жертву сведений. Для этого используются интимные фотографии, видеоизображения сексуального характера, которые пользователь хранил на своих страницах в соцсетях или в электронных почтовых ящиках [17, с. 107]. Вымогатель осуществляет так называемый «взлом» (неправомерный доступ) аккаунта, владельца или его e-mail, а далее, получив доступ к виртуальной учетной записи, шантажируют распространением интимных материалов среди его подписчиков [18, с. 27]. Распространённым стал и еще один способ использования интимных фотографий жертвы, который не требует применять несанкционированный доступ к личной странице потерпевшего. Их отправляют сами жертвы неизвестным в мессенджерах. Так, несовершеннолетняя студентка из Москвы отправила незнакомому молодому человеку, с которым переписывалась в Telegram, свои обнаженные фото с интимными позами. Злоумышленник, шантажируя девушку путем угроз публикации интимных снимков в Сети, склонил ее к занятию проституцией для отработки «долга». Оказав сексуальную услугу трем мужчинам, она передала сутенеру 20 тыс. руб., который стал вымогать уже 300 тыс. руб. И только тогда потерпевшая обратилась в полицию[3].

Новым видом вымогательства посредством цифровых средств коммуникации является sextortion, когда любителей порно шантажируют обнародованием записи с веб-камер сайта, на котором они смотрят запрещенный контент (даже в режиме «Инкогнито»). Вымогатели уверяют, что взломали устройство, получив доступ к камере, и записали «шалости» жертвы во время просмотра порно. В доказательство намерений на электронную почту жертвы отправляются письма с видеозаписью с сайта с «клубничкой». Для «выкупа» пикантных записей и требуется перевод денег[4].

[1] Приговор Петрозаводского городского суда Республики Карелия от 10.09.2020 по делу № 1-641 // Судебные и нормативные акты РФ: сайт. URL: https://sudact.ru/regular/doc/Uc2AsN33oD1R/ (дата обращения: 25.09.2023).

[2] Как мошенники получают наши персональные данные из банков? Объяснил эксперт // Аргументы и факты. URL: https://aif.ru/money/mymoney/kak_moshenniki_poluchayut_nashi_personalnye_dannye_iz_bankov_obyasnil_ekspert (дата обращения: 17.09.2023).

[3] 16-летнюю девушку шантажом заставили заниматься проституцией в Москве // Мослента: сайт. URL: https://moslenta.ru/news/lyudi/16-letnyuyu-13-10-2023.htm?ysclid=loee3nxssc11177211 (дата обращения: 22.09.2023).

[4] Санитары порносайтов. Как аферисты вымогают деньги у любителей клубнички // LTFE: сайт. URL: https://life.ru/p/1232583?

Жертвами вымогателей становятся и проститутки, зарегистрированные на сайтах знакомств, в социальных сетях для поиска клиентов, бывшие проститутки и модели веб-каминга [19, с. 90]. Из фабулы изученных уголовных дел следует, что новые технологии позволяют преступникам идентифицировать аккаунты лиц, осуществляющих запрещенные виды деятельности. Так, получила распространение практика верификации профилей с личными данными проституток и вебкам-моделей, осуществляющих поиск клиентов на просторах Интернета [20, с. 164]. Скачав с персональной страницы профильного сайта фотографию «жрицы» (и «жрецов») плотской любви, злоумышленники при помощи специальных программ «пробивают» личные данные жертвы. А далее выдвигается требование об уплате потерпевшим определённой суммы денег, чтобы избежать огласки в социуме участия в секс-бизнесе и репутационных потерь. Так, в одной из социальных сетей на аккаунт К. поступило сообщение с требованием о переводе 15 тыс. руб. Преступник сообщал, что в случае отказа заплатить деньги он разместит в пабликах видеозапись с ее интимным изображением. Студентка ранее занималась виртуальным моделингом, т. е. позировала за плату в обнаженном виде в закрытом ресурсе в Интернете. Вымогатели нашли ее аккаунт через специальную программу, позволяющую идентифицировать человека по его изображению[1].

Способы вымогательства преступниками модернизируются, его технологии адаптируются под современную ситуацию в стране. Например, вымогатель регистрируется в больших пабликах, где комментируются актуальные проблемы политического и общественно значимого характера. Далее он обращается к участнику дискуссии в личном сообщении как сотрудник спецслужбы и уведомляет его о наличии в его публичных сообщениях признаков состава преступления (оскорбление чувств верующих, призывы к мятежу, экстремизм и др.) и предлагает за вознаграждение удалить «преступный пост». В случае отказа программа якобы «автоматически» передаст сведения о факте преступления в правоохранительные органы. Этот вид «бизнеса», по прогнозам экспертов, и в будущем получит свое развитие более высокими темпами.

Еще одним способом вымогательства, появившимся сравнительно недавно, стало требование выкупа за потерянную вещь. Злоумышленник находит в интернете объявление о потере паспорта, телефона, ключей и предлагает перевести вознаграждение за находку, иначе он их выбросит или продаст. Используют преступники и схему выманивания денег на сайтах с «пиратским» контентом, когда на экране компьютера появляется баннер с сообщением о совершении преступления. За отдельную плату предлагается не сообщать в МВД IP-адрес и личные данные нарушителя. Учитывая появление множества новых способов совершения вымогательства в Сети, теоретики указывают на изменение уголовно-правовой природы вымогательства. Так, Т. М. Лопатина указывает на то, что «условно-цифровое вымогательство с уголовно-правовых позиций характеризуется как имущественное и корыстное преступление, а с криминологических – как насильственное преступление и принуждение к действию. …С позиции механизма виктимогенной ситуации получается, что жертве предъявляется имущественное требование, исполнение которого носит якобы добровольный характер» [12, с. 23]. А потому ученые предлагают наделить диспозицию ч. 2 ст. 163 УК РФ (вымогательство) новым способом со-

ysclid=lofxym6b xj95373337 (дата обращения: 22.09.2023).

[1] «С тебя 15 тысяч»: вебкам-девушку шантажировали «голым» видео из приват-чата, а потом выложили его в сеть // Комсомольская правда. Новосибирск. URL: https://www.nsk.kp.ru/daily/27088/4161402/ (дата обращения: 02.10.2023).

вершения вымогательства – «совершенное с угрозой удаления, вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей» [1, с. 220].

Выводы

Проведенное исследование описывает далеко не все способы совершения преступлений против собственности, в связи с чем их анализ будет продолжен автором. Учитывая масштабы цифровизации с массовым переходом на площадки Глобальной сети деятельности по оказанию образовательных, медицинских, косметологических, банковских услуг и др., торговли, деятельности органов государственной власти, преступность трансформируется под современные реалии и актуализируется в новых способах преступного поведения. В условиях виртуализации общественных отношений имеет значение дополнение научных знаний, позволяющих дать оценку тенденциям корыстной киберпреступности, разрабатывать более эффективные и своевременные меры ее предупреждения, прогнозировать новые криминальные способы, влияющие на качественные изменения корыстной преступности в сети Интернет. Полученные результаты могут быть использованы и в целях виктимологической профилактики. Для того чтобы прогнозировать новые криминальные способы совершения корыстных преступлений, влияющие на качественные изменения всей преступности в сети Интернет, необходим постоянный криминологический мониторинг указанной группы преступлений. На основе полученных данных могут быть приняты решения по криминализации новых деяний или ужесточению уголовной ответственности. С учетом криминогенности сферы Интернета требуется содержательное изменение статистических форм учета преступлений против собственности, совершаемых с использованием цифровых технологий.

Список литературы

1. Юхименко Д. М.-К. Преступления против собственности с применением информационных технологий // Социальное управление. 2023. № 5. С. 218–229.

2. Комаров А. А. Интернет-мошенничество: проблемы детерминации и предупреждения. М.: Юрлитинформ, 2013. 184 с.

3. Мазур А. А. Актуальные проблемы предупреждения преступности в социальной сети Даркнет // Вестник Российского университета кооперации. 2018. № 3 (33). С. 125–129.

4. Елин В. М. Мошенничество в сфере компьютерной информации как новый состав преступления // Бизнес-информатика. 2013. № 2 (24). С. 70–76.

5. Иванова Л. В. Хищение с использованием информационных технологий: проблемы квалификации // Юридическая наука и правоохранительная практика. 2020. № 1 (51). С. 29–36.

6. Соловьев В. С. Преступность в социальных сетях интернета (криминологическое исследование по материалам судебной практики) // Криминологический журнал Байкальского государственного университета экономики и права. 2016. № 1. С. 60–72.

7. Новичков В. Е. Информационная среда обитания и её уголовно-правовая охрана // Известия Юго-Западного государственного университета. Серия: История и право. 2023. № 3(4). С. 93–106.

8. Сафонов В. Н., Андреев Д. В. «Мошенничество от пандемии»: новые способы хищений // Вестник Волжского университета им. В. Н. Татищева. 2022. Т. 1, № 2 (101). С. 177–184.

9. Салаев З. Р. К вопросу о способе мошенничества, связанного с оказанием оккультных и психологических услуг // Образование и право. 2019. № 5. С. 171–175.

10. Олефирова А. В., Рокутова Е. А. Инфоцыганство как явление в интернет-пространстве // Вестник науки. 2022. № 6 (51). С. 169–174.

11. Ревякин С. В. Проблемы раскрытия хищений, совершаемых посредством современных электронных средств коммуникации // Правопорядок: история, теория, практика. 2018. № 3 (18). С. 27–32.

12. Евтушенко И. И. Виктимологическая защита жертв дистанционных хищений // Виктимология. 2023. № 1. С. 78–88.

13. Сафонов В. Н., Харченко О. В. Криминологическое исследование мошенничества в сфере компьютерной информации на примере деятельности интернет-букмекерских контор // Журнал правовых и экономических исследований. 2021. № 4. С. 39–50.

14. Сынгаевский Д. В. Мошенничество в глобальной сети Интернет как объект виктимологического исследования // Современный юрист. 2013. № 4. С. 136–144.

15. Шут О. А. Мошенничество в социальных сетях и способы его осуществления // Вестник Омского университета. Серия: Право. 2020. № 4. С. 97–106.

16. Простосердов М. А. Вымогательство, совершенное в сети Интернет // Библиотека криминалиста. 2013. № 6 (11). С. 150–152.

17. Ильницкий А. С. Криминологические риски интимной коммуникации в сети Интернет // Гуманитарные, социально-экономические и общественные науки. 2021. № 9. С. 106–109.

18. Родивилин И. П. Типологизация лиц, совершающих преступления в сфере компьютерной информации, по способу преступного деяния // Научный вестник Омской академии МВД России. 2017. № 4 (67). С. 25–29.

19. Алихаджиева И. С. Криминологические риски персональных данных: основные тенденции и прогнозы // Известия Юго-Западного государственного университета. Серия: История и право. 2023. № 13(3). С. 90–101.

20. Алихаджиева И. С. О новых тенденциях современной секс-индустрии и ее криминологических рисках // Актуальные проблемы российского права. 2021. Т. 16, № 4. С. 160–173.

21. Лопатина Т. М. Условно-цифровое вымогательство, или кибершантаж // Журнал российского права. 2015. № 1 (217). С. 118–126.

References

1. Yukhimenko D. M.-K. Prestupleniya protiv sobstvennosti s primeneniem informacionnyh tekhnologij [Crimes against property using information technology]. *Social'noe upravlenie = Social management*, 2023, no. 5, pp. 218–229.

2. Komarov A. A. Internet-moshennichestvo: problemy determinacii i preduprezhdeniya [Internet fraud: problems of determination and warning]. Moscow, Yurlitinform Publ., 2013. 184 p.

3. Mazur A. A. Aktual'nye problemy preduprezhdeniya prestupnosti v social'noj seti Darknet [Actual problems of crime prevention in the social network Darknet]. *Vestnik Rossiiskogo universiteta kooperatsii = Vestnik of the Russian University of Cooperation*, 2018, no. 3 (33), pp. 125–129.

4. Elin V. M. Moshennichestvo v sfere komp'yuternoj informacii kak novyj sostav prestupleniya [Fraud in the field of computer information as a new corpus delicti]. *Biznes-informatika = Business informatics*, 2013, no. 2 (24), pp. 70–76.

5. Ivanova L. V. Hishchenie s ispol'zovaniem informacionnyh tekhnologij: problemy kvalifikacii [Theft using information technologies: problems of qualification]. *Yuridicheskaya nauka i pravoohranitel'naya praktika = Legal science and law enforcement practice*, 2020, no. 1 (51), pp. 29–36.

6. Solov'ev V. S. Prestupnost' v social'nyh setyah interneta (kriminologicheskoe issledovanie po materialam sudebnoj praktiki) [Crime on social networks of the Internet (criminological research on the materials of judicial practice)]. *Kriminologicheskij zhurnal Bajkal'skogo gosudarstvennogo universiteta ekonomiki i prava = Criminological Journal of the Baikal State University of Economics and Law*, 2016, no. 1, pp. 60–72.

7. Novichkov V. E. Informacionnaya sreda obitaniya i eyo ugolovno-pravovaya ohrana [Information Habitat and its Criminal Law Protection]. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Seriya: Istoriya i pravo = Proceedings of the Southwest State University. Series: History and Law*, 2023, no. 13(4), pp. 93–106.

8. Safonov V. N., Andreev D. V. "Moshennichestvo ot pandemii": novye sposoby hishchenij ["Fraud from a pandemic": new methods of theft]. *Vestnik Volzhskogo universiteta im. V. N. Tatishcheva = Bulletin of the Volga University named after V. N. Tatishchev*, 2022, vol. 1, no. 2 (101), pp. 177–184.

9. Salaev Z. R. K voprosu o sposobe moshennichestva, svyazannogo s okazaniem okkul'tnyh i psihologicheskih uslug [To the question of the method of fraud related to the provision of occult and psychological services]. *Obrazovanie i pravo = Education and law*, 2019, no. 5, pp. 171–175.

10. Olefirova A. V., Rokutova E. A. Infocyganstvo kak yavlenie v internet-prostranstve [Infotsyganism as a phenomenon in the Internet space]. *Vestnik nauki = Bulletin of Science*, 2022, no. 6 (51), pp. 169–174.

11. Revyakin S. V. Problemy raskrytiya hishchenij, sovershaemyh posredstvom sovremennyh elektronnyh sredstv kommunikacii [Problems of disclosure of embezzlement committed through modern electronic means of communication]. *Pravoporyadok: istoriya, teoriya, praktika = Law and order: history, theory, practice*, 2018, no. 3 (18), pp. 27–32.

12. Evtushenko I. I. Viktimologicheskaya zashchita zhertv distancionnyh hishchenij [Victimoiogical Protection Victims of Remote Theft]. *Viktimologiya = Victimology*, 2023, no. 10 (1), pp. 78–88.

13. Safonov V. N., Kharchenko O. V. Kriminologicheskoe issledovanie moshennichestva v sfere komp'yuternoj informacii na primere deyatel'nosti internet-bukmekerskih kontor [Criminological study of fraud in the field of computer information on the example of the activities of Internet bookmakers]. *Zhurnal pravovyh i ekonomicheskih issledovanij = Journal of Legal and Economic Research*, 2021, no. 4, pp. 39–50.

14. Syngaevsky D. V. Moshennichestvo v global'noj seti Internet kak ob"ekt viktimologicheskogo issledovaniya [Fraud in the global Internet as an object of victimological research]. *Sovremennyi yurist = Modern lawyer*, 2013, no. 4, pp. 136–144.

15. Shut O. A. Moshennichestvo v social'nyh setyah i sposoby ego osushchestvleniya [Fraud in social networks and methods of its implementation]. *Vestnik Omskogo universiteta. Seriya: Pravo = Bulletin of Omsk University. Series: Law*, 2020, no. 4, pp. 97–106.

16. Prostoserdov M. A. Vymogatel'stvo, sovershennoe v seti Internet [Internet Extortion]. *Biblioteka kriminalista = Criminalist's Library*, 2013, no. 6 (11), pp. 150–152.

17. Il'nickij A. S. Kriminologicheskie riski intimnoj kommunikacii v seti Internet [Criminological risks of intimate communication on the Internet]. *Gumanitarnye, social'no-ekonomicheskie i obshchestvennye nauki = Humanitarian, socio-economic and social sciences*, 2021, no. 9, pp. 106–109.

18. Rodivilin I. P. Tipologizaciya lic, sovershayushchih prestupleniya v sfere komp'yuternoj informacii, po sposobu prestupnogo deyaniya [Typologization of persons who commit crimes in the field of computer information, according to the method of a criminal act]. *Nauchnyj vestnik Omskoj akademii MVD Rossii = Scientific Bulletin of the Omsk Academy of the Ministry of Internal Affairs of Russia*, 2017, no. 4 (67), pp. 25–29.

19. Alihadzhieva I. S. Kriminologicheskie riski personal'nyh dannyh: osnovnye tendencii i prognozy [Criminological risks of personal data: main trends and forecasts]. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Seriya: Istoriya i pravo = Proceedings of the Southwest State University. Series: History and Law*, 2023, no. 13(3), pp. 90–101.

20. Alikhadzhieva I. S. O novykh tendentsiyakh sovremennoy seks-industrii i ee kriminologicheskikh riskakh [New Trends in the Modern Sex Industry and Its Criminological Risks]. *Aktualnye problemy rossiyskogo prava = Actual problems of Russian law*, 2021, no. 16(4), pp.160–173.

21. Lopatina T. M. Uslovno-tsifrovoe vymogatelstvo, ili kibershantazh [Conditional digital extortion, or cyber sabotage]. *Zhurnal rossiyskogo prava = Journal of Russian law*, 2015, no. 1 (217), pp. 118–126.

Информация об авторе / Information about the Author

Москальков Артем Владиславович, аспирант, Московский университет имени А. С. Грибоедова, г. Москва, Российская Федерация,
e-mail: 11amo@list.ru

Artem V. Moskalkov, Post-Graduate Student, Moscow University A. S. Griboedov, Moscow, Russian Federation,
e-mail: 11amo@list.ru