УГОЛОВНОЕ ПРАВО И КРИМИНОЛОГИЯ

Статья / Article

УДК / UDC 343 : 340.130.54
DOI 10.35231/18136230_2022_1_125

Имущественные преступления с использованием IT-технологий: криминологический аспект

Т. О. Бозиев[1], А. В. Коротков[2], М. Н. Сипягина[3]

[1,3]Государственный институт экономики, финансов, права и технологий, Гатчина, Российская Федерация

[2]Северо-Западный институт управления Российской академии народного хозяйства и государственной службы при Президенте РФ, Санкт-Петербург, Российская Федерация

В статье исследуется криминологический аспект имущественных преступлений с использованием IT-технологий в условиях роста их показателей.

Предпринята попытка синтезировать основные криминологические факторы, способствующие увеличению показателей IT-преступности, с целью уяснения возможных направлений уголовной политики. Отрицательные характеристики состояния криминогенного состояния в сфере IT-технологий выдвигают на первый план необходимость переориентации уголовной политики, создания единой системы предупредительно-профилактических мероприятий. В связи с этим, задачи по установлению, анализу и искоренению криминогенных факторов, способствующих увеличению IT-преступлений, приобретают особое значение. Исследование позволило выявить особенности факторов, способствующих увеличению числа имущественных преступлений с использований IT-технологий на фоне общего снижения показателей уровня преступности.

Аргументирована группа факторов, оказывающих влияние на рост имущественных преступлений с использованием IT-технологий; проанализированы вскрывшиеся проблемы виктимологического, группового характера развития IT-преступности, в том числе в местах лишения свободы.

Ключевые слова: имущественные преступления, IT-технологии, правовая статистика, факторы преступности, виктимность, соучастие, ФСИН, «колл-центр», уголовная политика.

Для цитирования: Бозиев Т.О., Коротков А.В., Сипягина М.Н. Имущественные преступления с использованием IT-технологий: криминологический аспект // Ленинградский юридический журнал. – 2022. – № 1 (67). – С. 125–138. DOI 10.35231/18136230_2022_1_125

Property crimes using IT technologies: criminological aspect

Taulan O. Boziev[1], Alexey V. Korotkov[2], Maya N. Sipyagina[3]

[1,3]State Institute of Economics, Finance, Law and Technology, Gatchina, Russian Federation

[2]North-West Institute of Management of the Russian Academy of National Economy and Public Administration under the President of the Russian Federation, St. Petersburg, Russian Federation

The article is devoted to the study of the criminological aspect of property crimes using IT technologies in the context of an increase in their indicators.

The authors attempted to synthesize the main criminological factors contributing to the increase in IT-crime indicators in order to understand possible directions of criminal policy. Negative characteristics of the state of the criminogenic state in the field of IT technologies highlight the need to reorient criminal policy, create a unified system of preventive measures. In this regard, the task of identifying, analysing and eradicating the criminogenic factors that contribute to the increase in IT-crimes is of particular importance. The study revealed the features of factors contributing to the increase in the number of property crimes using IT technologies against the background of an overall decrease in crime rates.

A group of factors influencing the growth of property crimes using IT technologies is argued; analyzed the revealed problems of the victimological, group nature of the development of IT crime, including in places of deprivation of liberty.

Key words: property crimes, IT technologies, legal statistics, crime factors, victimhood, complicity, FSIN, "call center," criminal policy.

For citation: Boziev, T.O., Korotkov, A.V., Sipyagina, M.N. (2022) Imushchestvennye prestupleniya s ispol'zovaniem IT tekhnologij: kriminologicheskij aspekt [Property crimes using IT technologies: criminological aspect]. *Leningradskij yuridicheskij zhurnal – Leningrad Legal Journal.* No 1 (67). pp. 125–138. (In Russian). DOI 10.35231/18136230_2022_1_125

Введение

Важным критерием существования любого государства является охрана законных интересов своих граждан, в том числе имущественных. Современное российское общество безальтернативно движется к цифровизации как концепции социально-экономического развития, связанной с

цифровыми технологиями, внедряемыми в разные сферы жизнедеятельности и призванные улучшить их качество. Поэтому, хотим мы этого или нет, информационные технологии (IT) – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов[1], это наше настоящее и будущее. Но в данном явлении мы наблюдаем процесс абберации, когда достижения науки и техники используются в преступных интересах. Ущерб от подобных преступлений приобретает все больший масштаб, и, как мы можем видеть на некоторых самых ярких примерах, угроза киберпреступности уже стала реальностью не только для отдельных финансовых и иных организаций, но целых государств [8, с. 19].

Статистические показатели роста IT-преступности на современном этапе

На фоне снижения уровня преступности в России в целом, в том числе и некоторых имущественных преступлений, зафиксирован рост так называемой IT-преступности. Киберпреступность и киберпреступники имеют некоторые общие черты с традиционными преступлениями и преступниками, но онлайн-среда предоставляет новые и уникальные возможности для традиционных преступников, а также создает новую категорию онлайн-преступников [3, с. 19–21].

По статистическим данным МВД России, за январь-декабрь 2020 г. число преступлений, совершенных с использованием информационно-телекоммуникационных технологий, возросло на 73,4%, в том числе с использованием сети Интернет – на 91,3%, при помощи средств мобильной связи – на 88,3%.[2] За семь месяцев 2021 г. произошло почти 320 тыс. киберпреступлений. Это на 16% больше, чем за тот же период в прошлом году. Около 127 тыс. преступлений совершены с использованием мобильной связи, 104 тыс. – с применением карт. Если в первом полугодии 2021 г. число киберпреступлений увеличилось на 20,3%, то за десять месяцев текущего года – на 8,1%.[3]

[1] Об информации, информационных технологиях и о защите информации: федер. закон от 27 июля 2006 г. № 149-ФЗ. [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 23.01.2021).
[2] МВД Российской Федерации. Официальный сайт. [Электронный ресурс]. URL: https://мвд.рф/reports/item/22678184/ (дата обращения: 22.01.2021).
[3] Число киберпреступлений в России. [Электронный ресурс]. https://www.tadviser.ru/index.php/ (дата обращения: 03.01.2022).

По данным Генеральной прокуратуры, наибольшее число преступлений в IT сфере приходится на мошенничество и кражу. Более четверти в структуре всех преступлений занимают киберпреступления. Так, за шесть месяцев было зарегистрировано 271,1 тыс. киберпреступлений, что составило 26,5 процента от всех преступлений в России. Почти в 40 тыс. случаев жертвами таких преступлений стали пенсионеры. Еще в 3,3 тыс. – несовершеннолетние, в 1,4 тыс. случаев – инвалиды I и II группы. В январе – июне 2021 г. в стране было зарегистрировано более 168,7 тыс. различных мошенничеств. Это на 10,7 тыс. больше, чем годом ранее[1].

Аналогичные сведения предоставляет судебный департамент. Так за 9 месяцев 2021 г. по возможным имущественным статьям, где использовались IT-технологии были осуждены: ч. 3 ст. 158 УК – 29 958 чел.; ст. 159.3 УК – 340; ст. 159.6 УК – 10[2].

Как сообщает газета «Коммерсант», за 2020 г. телефонные и онлайн-мошенники выманили у россиян около 150 млрд руб., при этом самыми распространенными способами мошенничества являлись звонки под видом различных финансовых организаций, предложение медицинских услуг, а также создание фейковых интернет-магазинов[3].

Основные криминогенные факторы, влияющие на распространение преступлений против собственности с использованием IT-технологий

Несмотря на многочисленные научные труды по проблеме борьбы с IT-преступлениями, все же, на наш взгляд, есть аспекты, требующие более пристального внимания. Учитывая интеграцию информационно-технических технологий в общественное сознание, необходимо обратиться к криминогенным факторам, которые способствуют быстрому распространению имущественных преступлений в данной сфере. Используя общенаучные методы: анализа и синтеза, логического метода, контент-анализа средств массовой информации; а также частно-научные методы:

[1] Генеральная прокуратура РФ. Портал правовой статистики. Официальный сайт. [Электронный ресурс]. URL: http:// crimestat.ru/analytics ; https://rg.ru/2021/08/04/genprokuratura-obnarodovala-dannye-kriminalnoj-statistiki.html (дата обращения: 03.01.2022).

[2] Судебный департамент при Верховном Суде РФ. Официальный сайт. [Электронный ресурс]. http://www.cdep.ru/index.php?id=79&item=5895 (дата обращения: 03.01.2022)

[3] Коммерсантъ. Официальный сайт [Электронный ресурс]. URL: https://www.kommersant. ru/doc/4627762 (дата обращения: 24.01.2021).

правовой психологии, правовой статистики, нами были поставлены задачи по изучению факторов, влияющих на рост IT-преступности, с целью определения направления по предупреждению и профилактике рассматриваемой преступности [2, с. 120]. Одним из вопросов актуальной повестки является очевидная необходимость пересмотра подходов к правовому регулированию отношений, реализующихся в цифровой реальности [5, с. 23–31]. Стоит отметить, что в настоящее время проблема уголовно-правового обеспечения информационной безопасности требует принятия новых правовых решений, обусловленных возникновением новых рисков и вызовов [1, с. 2–4]. В период бурного развития информационных технологий с их помощью могут быть совершены практически любые преступления [6, с. 35–41].

Процесс постоянного совершенствования технической оснащенности на основе современных информационных технологий лежит в основе многих IT-преступлений с имущественным контекстом. Современные коммуникационные устройства от телефонов, смартфонов до иных устройств, программное обеспечение к ним, обладают колоссальными возможностями по получению, передаче или хранению данных. Мобильность, в прямом смысле этого слова, сопутствующее состояние современного общества. Использование информационно-технических устройств позволяет находиться в общении, решать насущные проблемы практически из любого места, где есть возможность подключения к сотовой связи или Интернет. Все чаще происходит перенос делового и коммерческого общения в информационное поле.

Активно внедряется так называемый электронный документооборот, все больше появляется официальных электронных документов, предоставляющих права или освобождающих от обязанностей (электронный больничный, ОСАГО, диагностическая карта и т.д.) Из этого многообразия отдельно хочется выделить широкую сеть онлайн-услуг, предназначенных для упрощения жизнедеятельности в различных сферах. Надо признать, что человек современного общества – это «человек с телефоном». Причем он привык не только находиться в постоянном контакте со своими коллегами, друзьями, близкими, но и все свое существование переносит в интернет-общение, включая имущественные интересы (онлайн-магазины, переводы денежных средств, оплату товаров, услуг и т.д.). В последнее время некоторые банковские структуры для облегчения

процесса идентификации клиентов вводят новые формы, среди них биометрическая аутентификация – распознание по голосу. Конечно, это удобно, но несет определенные риски. Современные устройства звукозаписи позволяют обеспечить качественное воспроизводство голоса. Представляется, что криминал обязательно этим воспользуется, дело за малым – разработать методику получения искомого голоса клиента и установить, где это можно использовать.

В довершение сказанного необходимо отметить совершенствование технической оснащенности преступного мира – различные считыватели банковских карт, RFID-ридеры, чипы NFC для смартфонов, скриммеры, накладки, вирусное программное обеспечение, мобильные сканеры и многое другое. Все это многообразие преследует единственную цель – получить доступ к конфиденциальной информации о других лицах, физических или юридических.

Таким образом, мы наблюдаем в некотором роде соревнование, когда используются информационно-технические средства в разных целях, общественно полезных или преступных, и победителем выступает та сторона, чья техническая оснащенность и методы получения или сохранения данных являются более передовыми. И этот процесс вряд ли можно остановить, поскольку, во-первых, будет постоянно совершенствоваться процесс информационно-технической оснащенности; во-вторых, возникает конфликт между информационным комфортом и информационной безопасностью, и если будет финансовый интерес или некая потребность, то безопасность уйдет на второй план; в-третьих, уходят в прошлое традиционные способы оборота денежных средств, активно внедряются безналичные, информационно-технические формы. Следовательно, будет снижаться традиционный и появляться инновационный характер преступности.

Общая характеристика кибермошенничества в условиях распространения новой коронавирусной инфекции на территории Российской Федерации

Безусловно, увеличение числа IT-преступлений связано с карантином, возникшим на фоне пандемии коронавируса, что вызвало длительную самоизоляцию граждан, прекращение работы предприятий, организаций, досуговых сфер, удаленную работу с использованием интернет-ресурсов. По данным РБК, всего с апреля по июнь прокуратура

зафиксировала 82,5 тыс. случаев мошенничества, в том числе больше двух третей (71%) по телефону или через Интернет. В аналогичный период прошлого года с помощью средств телекоммуникации совершалось только 50% мошенничеств, показывает статистика Генпрокуратуры. Это указывает на то, что общий прирост обеспечили именно эти способы обмана. В два раза увеличилось число преступлений по ст. 159.3 УК РФ (мошенничество с использованием электронных средств платежа)[1]. В России из-за пандемии в полтора раза выросло число ИТ-преступлений. Об этом стало известно 12 октября 2021 г. По словам министра Колокольцева, основную часть таких правонарушений составляет мошенничество, но также сюда входит распространение наркотиков[2].

Распространение COVID-19 привело к резкому росту кибермошенничества в весьма неожиданном секторе – доставке товаров, приобретенных через Интернет. Пользуясь ограничениями, связанными с самоизоляцией, мошенники похищают деньги и данные банковских карт пользователей с помощью фальшивых сайтов популярных курьерских служб. Специалисты Group-IB уже направили на блокировку более 250 фишинговых ресурсов [4, с. 37–42].

Действительно, в тот период, да и в настоящее время, активная жизнь населения перенеслась в интернет-пространство, что незамедлительно способствовало появлению различных мошеннических схем, фишинга. Появились ложные онлайн-площадки, сайты-клоны, позволяющие получать доступ к банковским реквизитам, счетам. Усилилось внедрение вредоносных программ, способствующих массовой утечке информации о реквизитах клиентов банка. Таким образом, введенный дефицит общения, ограничивающий легальные возможности и потребности, автоматически порождает ложные предложения в их реализации с единственной целью – заполучить доступ к финансам граждан, организаций. К сожалению, в этот период криминал работал на опережение, показав умение преобразовывать сложившуюся ситуацию в преступных целях.

[1] РБК. Официальный сайт. [Электронный ресурс]. URL: https://www.rbc.ru/society/31/08/2020/5f48ea169a79477e21e25d9d (дата обращения: 23.01.2021).

[2] Число киберпреступлений в России. [Электронный ресурс]. https://www.tadviser.ru/index.php/ (дата обращения: 03.01.2022).

Основные факторы, способствующие развитию IT-преступности

Необходимо остановиться на таком свойстве личности, как виктимность. Резкий переход на IT-отношения увеличивают вероятность того, что человек станет жертвой этих преступлений. В этой ситуации любой член общества потенциально виктимен при полном отсутствии с его стороны виктимного поведения [10, с. 33–80].

К сожалению, не все население обладает достаточной грамотностью в сфере IT-технологий, и как следствие, не может разобраться с многообразием информационных предложений на рынке. Прежде всего под данную категорию подпадает старшее поколение, которому сложно привыкнуть к существующим реалиям: незнание устройств, боязнь сделать что-то не так заставляет обращаться к незнакомым людям за помощью, полагаться на них. Лица в возрасте обладают повышенной внушаемостью и доверчивостью. Их легче обмануть и получить либо необходимую информацию, либо непосредственно денежные средства. Они становятся первыми жертвами имущественных преступлений, пытаясь хоть как-то получить требуемую услугу, и преступники часто пользуются этой ситуацией. Представляется, что также нельзя исключать из числа жертв и более молодое поколение, а также так называемых «продвинутых пользователей». Завышенная самооценка своих возможностей притупляет бдительность и внимательность, что может привести к неприятным последствиям имущественного характера. Например, обращение к подозрительным сайтам, приобретая необходимый онлайн-продукт (товары, заказы, бронирование мест отдыха и т.д.). Невнимательность к сообщениям мобильного банка тоже может привести к хищению средств с платежной карты. Так, часто преступники, получив коды платежной карты, сначала снимают небольшую сумму и отслеживают реакцию владельца, если карта не блокируется, то они снимают оставшуюся сумму денег, также через онлайн-магазин. К факторам виктимного поведения можно отнести так называемую «информационную рассеянность», когда жертвы увлечены чем-то конкретным в сети Интернет и не обращают внимания на происходящее вокруг.

В последнее время через СМИ очень часто публикуют сообщения предупредительного характера о новых мошеннических схемах. Но все равно, количество доверчивых граждан не уменьшается.

Следующий фактор, обусловивший IT-преступность – это высокая латентность. Данные преступления, как правило, технически сложны, следовательно, трудны в раскрываемости. Это понимают как жертвы, так и правоохранительные органы, поэтому не предпринимают активных действий для обращения или регистрации. В результате официальный уровень IT преступности ниже, чем реальное состояние, причем без учета стадий совершения неоконченных преступлений. Как известно, данная позиция лишь усугубляет ситуацию борьбы с преступностью в государстве. Представляется, что каждый человек в стране, так или иначе, сталкивался с IT-преступлениями, хотя бы на стадии приготовления или покушения к хищению.

Также нельзя не отметить, что рассматриваемые преступления совершаются в групповом исполнении, как правило, в сложном соучастии, хотя может быть и соисполнительство, когда одновременно требуется участие нескольких лиц, которые совместно выполняют часть объективной стороны IT хищения. Формы соучастия могут быть различные – это может быть группа лиц по предварительному сговору, организованная группа, преступная организация. Данный фактор обусловлен необходимостью специальных познаний в различных сферах – программирование, инженерия, материаловедение, банковское дело, психология и т.д. Причем участники группы могут выполнять свою часть преступного деяния удаленно, связываться между собой по электронным средствам коммуникации и не знать друг друга в лицо.

Представляется, что на этом фоне необходимо выделить так называемые «колл-центры» находящиеся в местах лишения свободы. Очевидно, что данная преступная деятельность носит организованный характер. Преступный мир руководствуется известным приемом – использовать место, где никогда не будут искать, т. е. в исправительных учреждениях. При этом мы видим только верхушку айсберга. Для «нормального» функционирования «колл-центров» требуются: финансирование, информационно-технические знания и оборудование (подмена номера), психологическая подготовка (вплоть до гипноза), знание предмета разговора (владение специальной терминологией), представление о работе учреждений, которыми они представляются, их особенности. Если обратить внимание на статистику судебного департамента, то лиц с высшим образованием среди осужденных за имущественные преступления с использованием информационных технологий не так уж много, в основном это лица со средним профессиональным либо общим

образованием. Следовательно, есть лица, которые не отбывают наказания, т. е. находятся вне уголовно-исправительной системы. Они обеспечивают осужденных необходимыми знаниями и умениями, психологическими методами и методикой работы структур, функции которых будет в дальнейшем дублироваться. Важным компонентом рассматриваемой деятельности выступает обеспечение «трудящихся в колл-центрах» средствами IT-коммуникаций. Согласно п. 17 Приложения 1 Правил внутреннего распорядка исправительных учреждений, утвержденных приказом Министерства юстиции РФ от 16 декабря 2016 г. № 295, средства мобильной связи и коммуникации, либо комплектующие к ним, обеспечивающие их работу, относятся к перечню вещей и предметов, продуктов питания, которые осужденным запрещается изготавливать, иметь при себе, получать в посылках, передачах, бандеролях либо приобретать. Если ориентироваться на информацию ФСИН, то самым распространенным способом доставки средств мобильной коммуникации осужденным является их переброс через ограждение с использованием различных способов[1], от традиционных, например рогатка, праща, приученные животные, до современных способов, например использование квадрокоптера. Также нельзя исключать вовлеченность некоторых сотрудников ФСИН в данную преступную схему, что существенно облегчает процесс оснащенности осужденных как техническими средствами, так и методическими материалами. Об этом свидетельствуют многочисленные публикации с СМИ и на телевидении. Конечно, равнять под одну гребенку абсолютно всех сотрудников не годиться, но факт остается фактом. Реакция на эти события со стороны ФСИН уже последовала: одна из приоритетных задач – обеспечить пресечение деятельности «колл-центров» и оборота средств мобильной коммуникации.

Подобные «колл-центры» организованы и развернуты в русскоговорящем сегменте ближнего зарубежья, с аналогичной оснащенностью и методикой. Складывается впечатление, что это звенья одной цепи и имущественная IT-преступность стала входить в транснациональную преступность со всеми выходящими последствиями. Детерминанты мошенничества и других преступлений, совершаемых с использованием электронных средств платежа, эволюционируют, приобретая глобальный масштаб и определяя особенности противоправного поведения вне зависимости от национальных инструментов по противодействию ему [9, с. 64–67].

[1] РИА новости. Официальный сайт. [Электронный ресурс]. URL: https://ria.ru/20200724/1574847335.html (дата обращения: 22.01.2021).

Нельзя обойти вниманием правовые факторы, способствующие развитию IT-преступности. Прежде всего в данном вопросе необходимо обратить внимание на общую тенденцию правового нигилизма, особенно в киберпространстве. До конца не разработан надежный алгоритм исполнения действующего законодательства. Например, не в полной мере работает закон о защите персональных данных, идут утечки персональных информаций о гражданах. В этой сфере не контролируется Интернет, где граждане часто для получения услуги вынуждены оставлять свои данные, которые впоследствии используются в преступных целях. К сожалению, государственные структуры (правоохранительные органы, ЦБ и др.) выступают лишь фиксаторами появления новых мошеннических схем, что объясняется безликостью и всеобъемлющей масштабностью интернет-пространства, затрудняющей борьбу с преступными проявлениями. Также нельзя не указать на общую неподготовленность правоохранительных органов к противодействию IT-преступности. Одной из причин выступает то, что потребность в специалистах по кибербезопасности, программированию в коммерческих структурах очень высока и оплата труда тоже соответствующая. Поэтому государственные структуры формируются по остаточному признаку.

Постановление Пленума Верховного Суда от 30.11.2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» в целом обеспечивает единообразные подходы в спорных вопросах квалификации. Вместе с тем ряд положений требуют некоторых уточнений, что будет способствовать предупреждению распространения рассматриваемых преступлений на стадиях неоконченного преступления. В уголовном законодательстве к имущественным преступлениям с использованием IT-технологий с определенной долей уверенности, можно отнести: ст. 159; 159.3; 159.6, п. «г» ч. 3 ст. 158 УК РФ. Конечно, отдельные элементы с использованием информационных познаний могут фигурировать и в других составах преступлений, что выходит за рамки нашего исследования. Так, в ППВС говорится о том, что «если обман не направлен непосредственно на завладение чужим имуществом, а используется только для облегчения доступа к нему, действия виновного в зависимости от способа хищения образуют состав кражи или грабежа», Действительно, применительно к нашему вопросу обман следует рассматривать не только как способ хищения в мошенничестве (ст. 159, 159.3, 159.6 УК РФ), но и как способ получения необходимой конфиденциальной информации для

дальнейшего совершения кражи (п. «г» ч. 3 ст. 158 УК РФ). Обман находится за рамками объективной стороны мошенничества в сфере компьютерной информации, относится к подготовительной стадии хищения и, соответственно, на квалификацию деяния не влияет [10, с. 40–48]. Поэтому, если лицо получило доступ к информации платежных карт, однако по не зависящим от него обстоятельствам ими не воспользовалось, содеянное следует квалифицировать как приготовление к мошенничеству (ст. 159, 159.3 УК РФ) или краже (п. «г» ч. 3 ст. 158 УК РФ).

Заключение

Подведя итог вышесказанному, можно сказать, что на наш взгляд, имущественные преступления с использованием IT-технологий выходят на новый, интенсивный путь развития, с элементами транснациональной преступности. В целях борьбы с данным явлением необходимо пересмотреть приоритеты уголовной политики, сконцентрировав внимание на правовых, процессуальных и уголовно-исполнительных аспектах. Представляется, что для снижения криминальной активности потребуется комплексный социальный и информационно-технический подход. Социальный подход – мотивация общества на систему информационной безопасности. Информационно-технический подход – на систему, препятствующую получению криминалом денежных средств (например, банки переводят денежные средства продавцу интернет-магазина только после подтверждения покупателя о получении товара или услуги). Можно согласиться с инициативой Общероссийского народного фронта, который предложил для защиты граждан пожилого возраста от интернет-мошенничества, предусмотреть возможность добровольного отказа от онлайн-платежей и переводов.

Список литературы

1. Авдеев В.А., Авдеева О.А. Основные направления совершенствования правовой политики по обеспечению в условиях глобализации информационной безопасности // Российская юстиция. – 2021. – № 3. – С. 2–4.

2. Алауханов Е. О. Криминология. – СПб.: Юридический центр-Пресс, 2013. – 606 с.

3. Далгалы Т.А. Киберкриминология: вызовы XXI века // Российская юстиция. – 2020. – № 10. – С. 19–21.

4. Денисов Н.Л. Негативные изменения киберпреступности в период пандемии и пути противодействия им // Безопасность бизнеса. – 2020. – № 4. – С. 37–42.

5. Крайнова Н.А. Права и технологии в сфере противодействия киберугрозам // Право и цифровая экономика. – 2021. – № 2. – С. 23–31.

6. Лавицкая М.И., Крапчатова И.Н. Структурно-содержательная характеристика главы 28 УК РФ: юридико-технические и правореализационные проблемы составов преступлений в сфере компьютерной информации // Российский следователь. – 2021. – № 6. – С. 35–41.

7. Лебедева А.А. Актуальные вопросы квалификации мошенничества в сфере компьютерной информации // Безопасность бизнеса. – 2018. – № 5. – С. 40–48.

8. Линников А.С. Экономические последствия расширения масштабов киберпреступности в России и мире // Банковское право. – 2017. – № 5. – С. 19–29.

9. Лютов В.А. Основные детерминанты мошенничества и других преступлений, совершенных с использованием электронных средств платежа, в России и Китае // Российский следователь. – 2021. – № 9. – С. 64–67.

10. Ривман Д.В. Криминальная виктимология. – СПб.: Питер, 2002. – 304 с.

References

1. Avdeev, V.A., Avdeeva, O.A. (2021). Osnovnye napravleniya sovershenstvovaniya pravovoj politiki po obespecheniyu v usloviyah globalizacii informacionnoj bezopasnosti [The main directions for improving the legal policy on ensuring information security in a globalized environment]. *Rossijskaya yusticiya – Russian Justice*. No 3. pp. 2–4. (In Russian).

2. Alauhanov, E.O. (2013). Kriminologiya [Criminology]. St. Peterrsburg: YUridicheskij centr-Press. 606 p. (In Russian).

3. Dalgaly, T.A. (2020). Kiberkriminologiya: vyzovy XXI veka [Cybercriminology: challenges of the 21st century]. *Rossijskaya yusticiya – Russian Justice.* No 10. pp. 19–21. (In Russian).

4. Denisov, N.L. (2020). Negativnye izmeneniya kiberprestupnosti v period pandemii i puti protivodejstviya im [Negative changes in cybercrime during the pandemic and ways to counter them]. *Bezopasnost' biznesa – Business security*. No 4. pp. 37–42. (In Russian).

5. Krajnova, N.A. (2021). Prava i tekhnologii v sfere protivodejstviya kiberugrozam [Rights and technologies in the field of countering cyber threats]. *Pravo i cifrovaya ekonomika – Law and the digital economy*. No 2. pp. 23–31. (In Russian).

6. Lavickaya, M.I., Krapchatova, I.N. (2021). Strukturno-soderzhatel'naya harakteristika glavy 28 UK RF: yuridiko-tekhnicheskie i pravorealizacionnye problemy sostavov prestuplenij v sfere komp'yuternoj informacii [Structural and substantive characteristics of chapter 28 of the Criminal Code of the Russian Federation: legal, technical and legal problems of the corpus delicti in the field of computer information]. *Rossijskij sledovatel' – Russian investigator.* No 6. pp. 35–41. (In Russian).

7. Lebedeva, A.A. (2018). Aktual'nye voprosy kvalifikacii moshennichestva v sfere komp'yuternoj informacii [Topical issues of qualification of fraud in the field of computer information]. *Bezopasnost' biznesa – Business security.* No 5. pp. 40–48. (In Russian).

8. Linnikov, A.S. (2017). Ekonomicheskie posledstviya rasshireniya masshtabov kiberprestupnosti v Rossii i mire [Economic consequences of the expansion of cybercrime in Russia and the world]. *Bankovskoe parvo – Banking law*. No 5. pp. 19–29. (In Russian).

9. Lyutov, V.A. (2021). Osnovnye determinanty moshennichestva i drugih prestuplenij, sovershennyh s ispol'zovaniem elektronnyh sredstv platezha, v Rossii i Kitae [The main determinants of fraud and other crimes committed using electronic means of payment in Russia and China]. *Rossijskij sledovatel' – Russian investigator*. No 9. pp. 64–67. (In Russian).

10. Rivman, D.V. (2002). *Kriminal'naya viktimologiya – Criminal victimology*. St. Petersburg: Piter. 304 p. (In Russian).

Вклад соавторов

Соавторство неделимое

Author contributions

Co-authorship indivisible

Об авторах

Бозиев Таулан Османович, кандидат юридических наук, доцент**,** Государственный институт экономики, финансов, права и технологий, Гатчина, Российская Федерация, ORCID ID: 0000-0002-4699-8326, e-mail: boziev1975@yandex.ru

Коротков Алексей Викторович, кандидат юридических наук, доцент**,** Северо-Западный институт управления Российской академии народного хозяйства и государственной службы при Президенте РФ, Санкт-Петербург, Российская Федерация, ORCID ID: 0000-0002-3629-5379, e-mail: 1964KAV@mail.ru

Сипягина Майя Николаевна, кандидат юридических наук, доцент**,** Государственный институт экономики, финансов, права и технологий, Гатчина, Российская Федерация, ORCID ID: 0000-0003-3201-2527, e-mail: mayya12@yandex.ru.

About the authors

Taulan O. Boziev, Cand. Sci. (Law), Assistant Professor, State Institute of Economics, Finance, Law and Technology, Gatchina, Russian Federation, ORCID ID: 0000-0002-4699-8326, e-mail: boziev1975@yandex.ru

Alexey V. Korotkov, Cand. Sci. (Law), Assistant Professor, North-West Institute of Management of the Russian Academy of National Economy and Public Administration under the President of the Russian Federation, St. Petersburg, Russian Federation, ORCID ID: 0000-0002-3629-5379, e-mail: 1964KAV@mail.ru

Maya N. Sipyagina, Cand. Sci. (Law), Assistant Professor, State Institute of Economics, Finance, Law and Technology, Gatchina, Russian Federation, ORCID ID: 0000-0003-3201-2527, e-mail: mayya12@yandex.ru

Поступила в редакцию: 09.02.2022 Received: 09 February 2022

Принята к публикации: 28.02.2022 Accepted: 28 February 2022

Опубликована: 30.03.2022 Published: 30 March 2022