DOI: 10.17803/1994-1471.2024.168.11.106-113

М. М. Долгиева*

Квалификация дипфейк-мошенничества и киберпохищения человека

Аннотация. Развитие технологий искусственного интеллекта закономерно влечет трансформацию цифровой преступности и появление совершенно новых, ранее не знакомых отечественному уголовному законодательству видов преступлений. Использование дипфейк-технологий при совершении мошенничества и так называемое киберпохищение человека (убеждение его под обманом покинуть место проживания и скрыться от родственников) с целью вымогательства выкупа за его «освобождение» являются совершенно новыми формами киберпреступности, общественная опасность которых признается на высшем законодательном уровне. Квалификация названных деяний по действующему уголовному закону является вынужденной и не в полной мере охватывает признаки состава преступления, в первую очередь его объективной стороны. В этой связи автором предлагаются два пути развития уголовного законодательства: введение уголовной ответственности за использование дипфейк-технологий при совершении посягательств на отношения собственности в отдельной норме закона либо в качестве квалифицирующих признаков имеющихся составов преступлений; публикация Пленумом Верховного Суда РФ разъяснения в части конкретизации способов совершения указанных преступлений и действий, входящих в объективную сторону незаконного лишения свободы, что позволит сформировать единообразную судебную практику.

Ключевые слова: искусственный интеллект; дипфейк; дипфейк-мошенничество; дипфейк-технологии; киберпохищение; виртуальное похищение человека; киберпреступность; цифровая преступность; квалификация кибермошенничества; интернет-вымогательство.

Для цитирования: *Долгиева М. М.* Квалификация дипфейк-мошенничества и киберпохищения человека // Актуальные проблемы российского права. — 2024. — Т. 19. — № 11. — С. 106–113. — DOI: 10.17803/1994-1471.2024.168.11.106-113.

Classification of Deepfake Fraud and Cyber Kidnapping

Madina M. Dolgieva, Dr. Sci. (Law), Senior Prosecutor, General Criminal Justice Department, Prosecutor General's Office of the Russian Federation, Justice Advisor, Moscow, Russian Federation
novator111@mail.ru

Abstract. The development of artificial intelligence technologies naturally entails the transformation of digital crime and the emergence of completely new types of crimes previously unknown to domestic criminal legislation. The use of deepfake technologies in committing fraud, as well as the so-called cyber kidnapping of a person (persuading him under deception to leave his place of residence and hide from his relatives) with the purpose of extorting a ransom for his «release» is a completely new form of cybercrime, the social danger of which is recognized at the highest legislative level. The classification of the above-mentioned acts under the current criminal law is of

* *Долгиева Мадина Муссаевна*, доктор юридических наук, старший прокурор Главного уголовно-судебного управления Генеральной прокуратуры Российской Федерации, советник юстиции
Большая Дмитровка ул., д. 15а, г. Москва, Россия, 125993
novator111@mail.ru

necessity and does not fully cover the elements of the crime, primarily its objective side. In this regard, the author proposes two ways of developing criminal legislation: the introduction of criminal liability for the use of deepfake technologies when committing encroachments on property relations in a separate provision of the law or as classifying features of existing bodies of crimes. The second option is an explanation by the Plenum of the Supreme Court of the Russian Federation as to specification of the methods of committing such crimes and actions as part of the objective side of illegal deprivation of liberty, which will make it possible to form a uniform judicial practice.
Keywords: artificial intelligence; deepfake; deepfake fraud; deepfake technologies; cyber kidnapping; virtual kidnapping; cybercrime; digital crime; cyber fraud classification; online extortion.
Cite as: Dolgieva MM. Classification of Deepfake Fraud and Cyber Kidnapping. *Aktual'nye problemy rossijskogo prava*. 2024;19(11):106-113. (In Russ.). DOI: 10.17803/1994-1471.2024.168.11.106-113.

«Киберпространство» — это концепция, занимающая центральное место в современной жизни общества и государства. Технологии позволили за очень короткое время произвести масштабные, фундаментальные и в то же время неблагоприятные изменения в некоторых отраслях экономики и права. Каждый день появляются новые продукты и услуги, основанные на уникальной коммуникационной инфраструктуре, в результате использования которой общество получает возможности, которые было трудно представить себе еще 20 лет назад. Инновации киберпространства принесли также беспрецедентное удобство связи, и темпы этих изменений продолжают удивительным образом ускоряться. При этом с глобальными положительными изменениями приходит не менее масштабная криминогенная составляющая. Число новых форм и методов цифровой преступности, активно эволюционировавшей в течение двух последних десятилетий, достигло огромного роста почти молниеносно, что теперь является новым предметом исследований науки уголовного права[1].

Внедрение инноваций в противоправную деятельность произошло стремительно. Сто́ит отметить, что два этих процесса развивались параллельно. Уже не удивляют правоприменителей преступления, совершаемые с использованием искусственного интеллекта — так называемых дипфейков[2]. В новостях почти ежедневно появляются истории о хищении денежных средств граждан путем мошенничества с использованием поддельных изображений и голоса знакомых им лиц, причем раскрываемость таких преступлений, мягко говоря, невысокая. Вопросы квалификации указанных деяний массово в науке права до настоящего времени не поднимались, несмотря на то, что существует относительная правовая неопределенность. Можно констатировать, что дипфейк — это одна из разновидностей цифровых (инновационных) средств совершения мошенничества в первую очередь.

В доктрине права тенденции киберпреступности рассматриваются в контексте прогрессирования IT-преступлений, усложнения и модификации применяемых преступных схем, роста числа мошеннических действий, а также использования информационных технологий террористическими и экстремистскими организациями, оборота оружия и боеприпасов, наркотических и психотропных веществ[3].

Впрочем, автора в нынешних цифровых реалиях заинтересовал также и такой новый вид преступлений против личности, как «похищение

[1] См.: *Васюков В. Ф., Волеводз А. Г., Долгиева М. М., Чаплыгина В. Н.* Преступления в сфере высоких технологий и информационной безопасности. М. : Прометей, 2023 ; *Долгиева М. М.* Криптопреступность в условиях специальной военной операции и западных санкций // Актуальные проблемы российского права. 2022. Т. 17. № 8 (141). С. 144–149.

[2] Дипфейк (от deep learning — «глубокое обучение» и fake — «подделка») — синтез правдоподобных поддельных изображений, видео и звука при помощи искусственного интеллекта.

[3] Противодействие преступлениям, совершаемым в сфере информационных технологий : учебник / под науч. ред. И. А. Калиниченко. М. : Инфра-М, 2023.

человека» с использованием сети Интернет без физического участия преступника. Так, в США в 2023 г. киберпреступники убедили подростка сбежать из дома, сообщив, что его семье угрожают. При этом по требованию виновных подросток направил родственникам фотографию, свидетельствующую о том, что его удерживают против воли, после чего родственники перечислили 80 тыс. долл. США «похитителям» за его освобождение[4]. Данное уголовное дело привлекло международное внимание, после чего такие случаи моментально распространились и на территории Российской Федерации[5].

Виртуальное похищение людей может принимать различные формы, в его основе лежит нестандартная схема вымогательства. Как правило, мошенники звонят кому-то и обманом заставляют заплатить выкуп за освобождение близкого человека, которого, по их мнению, похитили и которому угрожают. В отличие от традиционных похищений виртуальные похитители на самом деле никого не похищают. Вместо этого с помощью обмана и угроз они заставляют жертв быстро заплатить выкуп, прежде чем схема развалится.

Тем не менее сто́ит отметить разницу между двумя видами преступных действий: 1) мошенничество ограничивается телефонными переговорами с использованием дипфейков, и потерпевший успевает перечислить или передать денежные средства за освобождение родственника или за оказание ему помощи, и 2) когда мошенники идут дальше и работают в двух направлениях: убеждают человека уехать, спрятаться и поменять номера телефонов, параллельно требуя выкуп за его «освобождение» с родственников. При этом в обоих случаях виновные лица могут находиться как на территории, так и за пределами Российской Федерации.

С правовой точки зрения квалификация двух указанных деяний не может быть одинаковой. Если в первом случае это скорее классическое мошенничество (обман), то во втором — налицо более тяжкое преступление, к расследованию которого в связи с исчезновением человека подключается больше людей и средств.

На общественной опасности такого противоправного деяния хотелось бы остановиться подробнее. В частности, все случаи киберпохищения людей в Российской Федерации были совершены в отношении пожилых граждан, вынужденных скрываться по требованию киберпреступников в других регионах, опасаясь несуществующих угроз их жизни и здоровью. Некоторые из них лишались всех сбережений и брали кредиты, которые также перечислялись на счета преступников. Параллельно выдвигались требования об уплате выкупа их родственникам, а сотрудники правоохранительных органов были вынуждены осуществлять масштабные поиски человека с задействованием общественных организаций.

Очевидная наглость виновных лиц и их пренебрежение к правовой системе являются следствием слабой ответственности по уголовному законодательству России и причиной дальнейшего совершенствования криминальных инструментов более изощренных преступлений.

Роль киберпреступников в совершении новых видов преступлений становится всё более специализированной. Это прослеживается по распространению нелегального сегмента сети Интернет, предлагающего продажу личной и финансовой информации, так как получение кредита потерпевшими по требованию преступников или предоставление доступа к их счетам свидетельствуют о том, что жертва не является случайной. В этой связи сто́ит отметить, что указанные преступления посягают одновременно на несколько объектов уголовно-правовой охраны — как на безопасность личности, собственности, так и на безопасность информации.

Кроме того, современная цифровая преступность изменила само понятие места соверше-

[4] Виртуальное похищение // URL: https://www.usatoday.com/story/news/nation/2024/01/03/what-is-a-cyber-kidnapping/72095095007/ (дата обращения: 15.04.2024).

[5] Вам нужно срочно уехать: как телефонные мошенники вынуждают людей организовать собственное похищение // URL: https://vm.ru/accidents/1062550-vam-nuzhno-srochno-uehat-kak-telefonnye-moshenniki-vynuzhdayut-lyudej-organizovat-sobstvennoe-pohishenie (дата обращения: 15.04.2024).

ния преступления. Процесс развития законодательства не был установлен с учетом объема требований, предъявляемых к нему в настоящее время, или темпов, с которыми эти требования должны выполняться. Вместе с тем приверженность отечественного законодателя к обеспечению верховенства закона не допускает, чтобы инфраструктура, позволяющая совершать эти преступления, оставалась безнаказанной.

Как правильно отмечается в науке уголовного права, учение о фиксации доказательственной информации, используемой в интернет-пространстве, требует постоянных дополнений, в том числе с изучением опыта западных стран в области компьютерной криминалистики[6]. Так, в частности, в США сообщается, что ключевым моментом в расследовании киберпреступлений является всеобъемлющий доступ к электронным доказательствам: содержимому электронных писем, мгновенных сообщений, фотографиям, данным сервера, журналам сеансов, информации подписчиков и т.п., в том числе и в случаях, когда такая информация находится за пределами страны, что способствует развитию трансграничного обмена данными[7].

Впрочем, в условиях современного мира, когда Российская Федерация лишена возможности полноценного международно-правового сотрудничества[8], приходится формировать собственные механизмы расследования и раскрытия цифровых преступлений для защиты информации граждан, их собственности и личной безопасности.

Минцифры России совместно с МВД России и Роскомнадзором прорабатывает вопросы правового регулирования цифровой технологии подмены личности (дипфейк) в целях недопущения ее использования в противоправных целях, поскольку законом данная сфера никак не регламентируется[9]. Сами по себе создание и использование дипфейков не являются преступлением; в отечественной судебной практике уже имеется судебное решение о признании дипфейка объектом авторского права[10]. Вместе с тем, несмотря на то, что статистика преступлений, совершаемых с использованием данной технологии, не ведется, интерес законодателей к ее регулированию растет. В частности, в Государственной Думе ФС РФ высказано мнение о необходимости включения в перечень отягчающих обстоятельств, предусмотренный статьей 63 УК РФ, использование продуктов искусственного интеллекта при совершении преступлений, поскольку другие способы защиты граждан от дипфейков — это лишь косвенные меры. В свою очередь, другими представителями власти предлагается полностью регламентировать методику, которая позволяет подменять лица, тела, голоса на видеозаписи, фотографии или в видеопотоке, пока технологии не вышли из-под контроля[11]. Насколько успешными будут указанные законодательные инициативы, покажет время, однако в данный момент следует рассмотреть проблемы квалификации таких деяний с учетом действующего уголовного закона.

---

6 Расследование преступлений с использованием компьютерной информации из сети Интернет : учеб. пособие / под ред. д-ра юрид. наук, доц. А. Г. Волеводза. М. : Проспект, 2022.

7 Assistant Attorney General Brian A. Benczkowski Delivers Remarks at the «Justice in Cyberspace» Symposium // URL: https://www.justice.gov/opa/speech/assistant-attorney-general-brian-benczkowski-delivers-remarks-justice-cyberspace (дата обращения: 15.04.2024).

8 *Долгиева М. М., Долгиев М. М.* Двойные стандарты Совета Европы // Вестник Московского университета МВД России. 2022. № 5. С. 108–112.

9 Минцифры с МВД и Роскомнадзором определят наказание за дипфейки // URL: https://www.vedomosti.ru/technology/articles/2024/02/16/1020587-mintsifri-s-mvd-i-roskomnadzorom-opredelyat-nakazanie-za-dipfeiki (дата обращения: 15.04.2024).

10 Постановление Девятого арбитражного апелляционного суда по делу № А40-200471/2023 // URL: https://kad.arbitr.ru/Card/4d7f0305-69af-44fe-8841-a59e84aa7deb (дата обращения: 15.04.2024).

11 Наказание за преступления с использованием ИИ предлагают ужесточить // URL: https://pravo.ru/news/249001/ (дата обращения: 15.04.2024).

По мнению профессора Л. В. Головко, мошенничество остается таковым, независимо от способа обмана: он может быть вербальным, телефонным, сопряженным с созданием фейковых видео и т.п., это ничего не меняет в уголовно-правовом плане, в каких-то случаях даже не усложняя, а упрощая доказывание, так как доказать просто произнесенные и нигде не зафиксированные слова иногда сложнее, чем доказать подложность видео[12]. То есть существующее на сегодняшний день уголовное и уголовно-процессуальное законодательство, по его мнению, обладает всем необходимым инструментарием, чтобы бороться с любыми проявлениями мошенничества, такими как дипфейки или телефонные обманы.

Действительно, использование дипфейк-технологий в качестве средства или способа совершения мошенничества возможно квалифицировать в зависимости от действий по ст. 159.6 УК РФ как хищение путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей или просто как мошенничество по ст. 159 УК РФ.

Законодательное определение дипфейков, возможно, и было бы нелишним, однако его отсутствие не означает, что правоохранительные органы и суды не должны применять данный термин в документах. При этом использование искусственного интеллекта не может усиливать ответственность виновного лица и являться отягчающим обстоятельством, как это предлагалось выше, потому что цифровые технологии лишь видоизменяют средства и способы мошенничества, но не увеличивают его общественную опасность.

В свою очередь, преступления, связанные с киберпохищением людей, — это новое и очень опасное направление киберпреступности, с которым необходимо качественно бороться, в том числе и путем изменения законодательства. Так, Бутырским межрайонным следственным отделом Главного следственного управления Следственного комитета РФ по г. Москве расследуется уголовное дело по признакам преступлений, предусмотренных пунктом «а» ч. 2 ст. 127 УК РФ (незаконное лишение свободы), п. «б» ч. 3 ст. 163 УК РФ (вымогательство с целью получения имущества), в отношении неустановленных лиц, которые под обманным предлогом уговорили пожилую женщину покинуть ее постоянное место жительства и лишили возможности общения с родственниками. В рамках уголовного дела установлено, что женщина стала жертвой телефонных мошенников, которые склонили ее к передаче им крупной суммы денежных средств[13]. При этом, на наш взгляд, названная квалификация, ввиду общетеоретических определений незаконного лишения свободы и вымогательства, является вынужденной.

Объективная сторона преступления, предусмотренного статьей 127 УК РФ, выражается в действиях, состоящих в реальном лишении или ограничении личной свободы потерпевшего, не связанных с его похищением. То есть при совершении преступления виновное лицо физически должно выполнить объективную сторону деяния — либо самостоятельно удерживать потерпевшего, либо высказывать ему угрозы, под влиянием которых потерпевший находится в месте его удержания. Этот же смысл вкладывает в толкование действий виновного лица постановление Пленума Верховного Суда РФ от 24.12.2019 № 58 «О судебной практике по делам о похищении человека, незаконном лишении свободы и торговле людьми», определяя личное, а не дистанционное, участие виновного лица в незаконном удержании.

Собственно, в описываемом примере никаких угроз потерпевшей не высказывалось, а использовался только обман, под которым ее склонили самостоятельно покинуть место жительства и скрываться от родственников, вы-

[12] Мошенничество с использованием дипфейков доказать проще, чем обычный обман // URL: https://rapsinews.ru/digital_law_news/20231120/309397389.html (дата обращения: 15.04.2024).

[13] Следователи устанавливают местонахождение пожилой женщины, ставшей жертвой мошенников // URL: https://t.me/skmoscowgsu/1822 (дата обращения: 15.04.2024).

бросив все средства связи с ними. Допустимо ли в таком случае квалифицировать действия виновных по ст. 127 УК РФ, если фактически ими не была выполнена объективная сторона преступления, — вопрос спорный, однако при отсутствии других вариантов следует согласиться с позицией следственных органов, так как одним вымогательством действия виновных лиц не ограничивались. Налицо совокупность преступлений.

В судебной практике многократно высказывалась позиция (и ее можно считать устоявшейся), что при незаконном лишении свободы потерпевший не захватывается, не изымается из своей среды, не похищается, а остается на месте, но ограничивается в передвижении. При этом объективная сторона преступления выражается в совершении действий, состоящих в реальном лишении или ограничении личной свободы потерпевшего, не связанных с его похищением. То есть потерпевший незаконно, в принудительном порядке, помимо его воли удерживается в том месте, где он сам добровольно до этого находился, его лишают возможности передвигаться по своему усмотрению, общаться с другими людьми.

Киберпохищение человека в соответствии с толкованием ст. 126 УК РФ также нельзя прямо отнести к традиционно понимаемому похищению человека ровно по тем же основаниям — отсутствие фактических физических действий и личного участия виновного лица, несмотря на то, что умысел направлен именно на удержание человека до получения выкупа. Безусловно, наиболее подходящей является квалификация таких действий по ст. 127 УК РФ, поскольку потерпевший перемещается самостоятельно и добровольно, хотя и под действием обмана, что в свою очередь создает условия для последующего вымогательства.

Кроме того, необходимым критерием для юридической квалификации будут и момент формирования умысла на незаконное лишение свободы, доказанность этого умысла в совокупности с фактически совершенными действиями. Сто́ит отметить, что указанные действия по обманному перемещению человека могут с натяжкой составлять и объективную сторону вымогательства. В частности, в науке права высказывалось мнение о том, что преступление, предусмотренное статьей 127 УК РФ, является довольно простым и не вызывающим вопросов ввиду одноактности[14]. Вместе с тем, по мнению ряда ученых, если незаконное лишение свободы является способом совершить другое преступление, посягающее на другой объект (в данном случае как раз хищение денежных средств и вымогательство), то оно охватывается конструктивными признаками его состава и дополнительной квалификации по ст. 127 УК РФ не требует[15].

На наш взгляд, сложности анализируемого деяния, связанного с киберпохищением, должна соответствовать и сложная квалификация. В данном случае действия виновных, направленные на убеждение потерпевшего покинуть место проживания и скрываться от родственников, должны действительно дополнительно квалифицироваться как незаконное лишение свободы, т.к. очевидно, что для способа вымогательства эти действия слишком объемны.

Представляется, что в юридической литературе необходимо научно обосновать различные варианты квалификации как киберпохищения человека, так и преступлений, совершаемых с использованием дипфейков. При этом оба деяния могут совершаться одновременно, одно быть частью другого.

Так или иначе, увеличивающаяся общественная опасность указанных преступлений и трансформация видов преступной деятельности требуют срочной реакции если не законодателя, то научного сообщества однозначно. При таких обстоятельствах можно рассмотреть два пути

[14] *Полянская Е. М.* Объективные признаки незаконного лишения свободы (ст. 127 УК РФ) // Российский следователь. 2021. № 12. С. 54–58.

[15] Уголовное право Российской Федерации. Особенная часть : учебник / Ю. В. Грачева, Л. Д. Ермакова, Г. А. Есаков [и др.] ; под ред. Л. В. Иногамовой-Хегай, А. И. Рарога, А. И. Чучаева. 2-е изд., испр. и доп. М. : Контракт, Инфра-М, 2009.

адаптации уголовного законодательства к современным реалиям киберпреступности: кардинальный и более осторожный. К первому можно отнести введение уголовной ответственности (как это предлагается некоторыми депутатами) за использование технологий искусственного интеллекта при совершении преступлений против собственности в отдельной норме либо в качестве квалифицирующего признака таких преступлений. Второй путь, который представляется нам оптимальным, — это разъяснения Пленума Верховного Суда РФ (например, в постановлениях от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» и от 24.12.2019 № 58 «О судебной практике по делам о похищении человека, незаконном лишении свободы и торговле людьми»). В частности, такие разъяснения могут затронуть вопросы объективной стороны незаконного лишения свободы, к которой могут быть отнесены действия, связанные с обманом и убеждением потерпевшего покинуть место проживания, самостоятельно и добровольно, без помощи виновного лица скрываться от родственников, его нахождением в выбранном месте без средств связи без участия виновного лица. Кроме того, следует разъяснить, что обман и угрозы, высказываемые потерпевшему дистанционно с использованием информационно-коммуникационных технологий, также входят в объективную сторону состава незаконного лишения свободы.

Помимо этого, следует разъяснить, что применение технологий искусственного интеллекта (дипфейков) может являться способом совершения мошенничества или иного хищения имущества, причем в каждом конкретном случае необходимо устанавливать факт использования синтезированного голоса или изображения экспертным путем.

Предлагаемые меры позволят сформировать единообразную, а не фрагментарную судебную практику в вопросах противодействия киберпреступности, особенно в условиях недостающих правовых компетенций правоохранительной системы.

БИБЛИОГРАФИЯ

1. *Долгиева М. М., Долгиев М. М.* Двойные стандарты Совета Европы // Вестник Московского университета МВД России. — 2022. — № 5. — С. 108–112.
2. *Долгиева М. М.* Криптопреступность в условиях специальной военной операции и западных санкций // Актуальные проблемы российского права. — 2022. — Т. 17. — № 8 (141). — С. 144–149.
3. *Васюков В. Ф., Волеводз А. Г., Долгиева М. М., Чаплыгина В. Н.* Преступления в сфере высоких технологий и информационной безопасности. — М. : Общество с ограниченной ответственностью «Издательство Прометей», 2023. — 1086 с.
4. *Полянская Е. М.* Объективные признаки незаконного лишения свободы (ст. 127 УК РФ) // Российский следователь. — 2021. — № 12. — С. 54–58.
5. Противодействие преступлениям, совершаемым в сфере информационных технологий : учебник / под науч. ред. И. А. Калиниченко. — М. : Инфра-М, 2023. — 642 с.
6. Расследование преступлений с использованием компьютерной информации из сети Интернет : учеб. пособие / под ред. д-ра юрид. наук, доц. А. Г. Волеводза. — М. : Проспект, 2022. — 200 с.
7. Уголовное право Российской Федерации. Особенная часть : учебник / Ю. В. Грачева, Л. Д. Ермакова, Г. А. Есаков [и др.] ; под ред. Л. В. Иногамовой-Хегай, А. И. Рарога, А. И. Чучаева. — 2-е изд., испр. и доп. — М. : Контракт, Инфра-М, 2009. — 800 с.

Материал поступил в редакцию 20 апреля 2024 г.

REFERENCES (TRANSLITERATION)

1. Dolgieva M. M., Dolgiev M. M. Dvoynye standarty Soveta Evropy // Vestnik Moskovskogo universiteta MVD Rossii. — 2022. — № 5. — S. 108–112.
2. Dolgieva M. M. Kriptoprestupnost v usloviyakh spetsialnoy voennoy operatsii i zapadnykh sanktsiy // Aktual'nye problemy rossijskogo prava. — 2022. — T. 17. — № 8 (141). — S. 144–149.
3. Vasyukov V. F., Volevodz A. G., Dolgieva M. M., Chaplygina V. N. Prestupleniya v sfere vysokikh tekhnologiy i informatsionnoy bezopasnosti. — M.: Obshchestvo s ogranichennoy otvetstvennostyu «Izdatelstvo Prometey», 2023. — 1086 s.
4. Polyanskaya E. M. Obektivnye priznaki nezakonnogo lisheniya svobody (st. 127 UK RF) // Rossiyskiy sledovatel. — 2021. — № 12. — S. 54–58.
5. Protivodeystvie prestupleniyam, sovershaemym v sfere informatsionnykh tekhnologiy: uchebnik / pod nauch. red. I. A. Kalinichenko. — M.: Infra-M, 2023. — 642 s.
6. Rassledovanie prestupleniy s ispolzovaniem kompyuternoy informatsii iz seti Internet: ucheb. posobie / pod red. d-ra yurid. nauk, dots. A. G. Volevodza. — M.: Prospekt, 2022. — 200 s.
7. Ugolovnoe pravo Rossiyskoy Federatsii. Osobennaya chast: uchebnik / Yu. V. Gracheva, L. D. Ermakova, G. A. Esakov [i dr.]; pod red. L. V. Inogamovoy-Khegay, A. I. Raroga, A. I. Chuchaeva. — 2-e izd., ispr. i dop. — M.: Kontrakt, Infra-M, 2009. — 800 s.