ТЕОРИЯ И ПРАКТИКА ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

Александр Витальевич АРТЮХОВ,
кандидат юридических наук, ORCID 0000-0001-9344-5241
Волгоградская академия МВД России (г. Волгоград)
заместитель начальника кафедры оперативно-разыскной деятельности и специальной техники
alex.v.artuhov@yandex.ru

Александр Михайлович ЮРИН,
Главное управление МВД России по Волгоградской области (г. Волгоград)
начальник отдела по борьбе с противоправным использованием информационно-коммуникационных технологий
mvd34@mvd.gov.ru

Научная статья
УДК 343.985:(343.3/.7:004)

ОПЕРАТИВНО-РАЗЫСКНАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ, СОВЕРШЁННЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ ИЛИ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ
(НА ПРИМЕРЕ ПРАВОПРИМЕНИТЕЛЬНОЙ ПРАКТИКИ ВОЛГОГРАДСКОЙ ОБЛАСТИ)

КЛЮЧЕВЫЕ СЛОВА. Информационно-телекоммуникационные технологии, компьютерная информация, оперативно-разыскная деятельность, оперативно-разыскное мероприятие, киберпреступник, компьютерный вирус.

АННОТАЦИЯ. ***Введение.*** *В статье обосновывается необходимость использования гласных и негласных сил, средств и методов оперативно-разыскной деятельности в рамках противодействия органов внутренних дел преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации. Рассмотрены наиболее значимые элементы оперативно-разыскной характеристики таких преступлений: современное состояние преступности в сфере информационно-телекоммуникационных технологий; обстановка совершения преступления; оперативно значимые данные о личности киберпреступника и потерпевших; способы совершения преступления; оперативно-разыскная профилактика.* ***Методы.*** *При проведении исследования применялся общенаучный диалектический метод познания окружающей действительности, предполагающий полное и всестороннее изучение явлений, рассмотрение связей и противоречий между ними. Кроме того, были использованы метод описания и метод логического осмысления. Проведен анализ статистических данных, характеризующих современное состояние противодействия IT-преступлениям, а также личность киберпреступников.* ***Результаты.*** *В статье описаны существующие в настоящее время способы не только совершения преступлений рассматриваемого вида, но и оказания противодействия деятельности сотрудников оперативных подразделений по их выявлению, документированию и раскрытию. Представлен зарубежный опыт борьбы с IT-преступлениями. Сформулированы предложения по совершенствованию законодательства, регламентирующего оперативно-разыскную деятельность.*

ВВЕДЕНИЕ

В современном мире развитие информационно-телекоммуникационных технологий (далее – ИТТ) имеет по-настоящему глобальный характер. ИТТ пронизывают все сферы деятельности общества и государства, и доступность информационных систем непосредственно влияет на их широкое применение. Проблема поиска новых, эффективных путей противодействия преступлениям, совершаемым в сфере ИТТ (далее

Alexander V. ARTYUKHOV,
Cand. Sci. (Jurisprudence), ORCID 0000-0001-9344-5241
Volgograd Academy of the Ministry
of Interior of Russia (Volgograd, Russia)
Deputy Head of the Department of Operational
Investigative Activities and Special Equipment
alex.v.artuhov@yandex.ru

Alexander M. YURIN,
Main Directorate of the Ministry of Interior of Russia
for the Volgograd Region (Volgograd, Russia)
Head of the Department for Combating Illegal Use
of Information and Communication Technologies
mvd34@mvd.gov.ru

OPERATIONAL INVESTIGATIVE CHARACTERISTICS OF CRIMES COMMITTED USING INFORMATION AND TELECOMMUNICATION TECHNOLOGIES OR IN THE FIELD OF COMPUTER INFORMATION (BASED ON THE EXAMPLE OF LAW ENFORCEMENT PRACTICE IN THE VOLGOGRAD REGION)

KEYWORDS. Information and telecommunication technologies, computer information, operational investigative activities, operational investigative acts, cybercriminal, computer virus.

ANNOTATION. ***Introduction.*** *The article substantiates the need to use public and secret forces, means and methods of operational investigative activities as part of the internal affairs bodies' counteraction to crimes committed using information and telecommunication technologies or in the field of computer information. The most significant elements of the operational investigative characteristics of such crimes are considered: the current state of crime in the field of information and telecommunication technologies; the context of the crime; operationally relevant data on the identity of the cybercriminal and victims; methods of committing a crime; operational investigative prevention.* ***Methods.*** *When conducting the research, the general scientific dialectical method of cognition of the surrounding reality was used, which involves a complete and comprehensive study of phenomena, consideration of connections and contradictions between them. In addition, the description method and the logical comprehension method were used. An analysis of statistical data characterizing the current state of combating IT crimes, as well as the identity of cybercriminals, was carried out.* ***Results.*** *The article describes currently existing methods of not only committing crimes of this type, but also countering the activities of employees of operational units to identify, document and disclose them. Foreign experience in combating IT crimes is presented. Proposals have been formulated to improve the legislation regulating operational investigative activities.*

- IT-преступления), является одной из наиболее важных для государства, а потому постоянно находится в фокусе внимания его уполномоченных органов и должностных лиц. Именно вокруг организации противодействия IT-преступлениям во многом формируются программные нормативные документы, ориентированные на борьбу с преступностью и обеспечение безопасности страны. Неслучайно в Стратегии национальной безопасности Российской Федерации, утвержденной указом Президента Российской Федерации от 2 июля 2021 г. № 400, IT-преступления признаны одной из основных угроз общественной безопасности.

В теории оперативно-разыскной деятельности (далее – ОРД) методика противодействия преступлениям различных видов, в том числе и IT-преступлениям, наиболее полно освещается при раскрытии элементов их оперативно-разыскной характеристики. Она представляет собой одну из наиболее дискуссионных категорий в оперативно-разыскной науке. При этом споры вокруг нее ведутся по трем основным направлениям: о понятии, о содержании и об обусловленности существования. Считаем необходимым, прежде чем начать исследовать вопросы оперативно-разыскной характеристики IT-преступлений, рассмотреть имеющие отношение к ней теоретические вопросы.

Под оперативно-разыскной характеристикой преступлений следует понимать совокупность их свойств и информационных признаков, сведения о которых необходимы субъектам ОРД для предупреждения, выявления и раскрытия этих преступлений. Безусловно, приведенное определение можно называть абстрактным. Но мы в первую очередь стремились взглянуть на изучаемую категорию с семантической точки зрения, которая позволяет определить ее внешне выраженную сущность.

Необходимость существования элементов оперативно-разыскной характеристики преступлений обосновывается фактической невозможностью рассматривать данную категорию в общем порядке, без применения структурированного подхода. Очевидно, что содержательно оперативно-разыскная характеристика преступлений представляет собой достаточно объемный массив информации, использование которого без деления его на составные части весьма затруднительно. Это не приведет к пониманию сущности исследу-

Таблица 1.

Количество зарегистрированных в России IT-преступлений, 2021-2023 гг.

Период	Всего IT-преступлений	Тяжких и особо тяжких	С использованием сети Интернет	С использованием средств мобильной связи
2021 год	517,7 тыс. (+1,4%)	288,3 тыс. (+7,7%)	351,5 тыс. (+17,0%)	217,6 тыс. (-0,5%)
2022 год	522,1 тыс. (+ 0,8%)	272,2 тыс. (-5,6%)	381,1 тыс. (+8,4%)	213,0 тыс. (-2,1%)
2023 год	677,0 тыс. (+29,7%)	342,6 тыс. (+25,9%)	526,8 тыс. (+38,2%)	526,8 тыс. (+38,2%)

Таблица 2.

Количество IT-преступлений, зарегистрированных в Волгоградской области, 2021-2023 гг.

Период	Всего преступлений в сфере ИТТ или компьютерной информации	Динамика количества преступлений в сфере ИТТ или компьютерной информации	Приостановлено (из категории тяжких и особо тяжких преступлений)	Ущерб, тыс. руб.
2021 год	9 769	+1 206	7 797	1 299 134
2022 год	10 992	+1 223	6 942	925 256
2023 год	13 636	+2 644	8 532	1 871 600

емого феномена и не будет носить прикладного или гносеологического характера.

Обоснованность категории «оперативно-разыскная характеристика преступлений» – это, пожалуй, самый значимый дискуссионный вопрос, в рамках решения которого вносятся даже весьма радикальные предложения, ставящие под сомнение само существование оперативно-розыскной характеристики преступлений как самостоятельного явления. В чем же находят основу такие сомнения? С содержательной стороны оперативно-разыскная характеристика преступлений достаточно сильно схожа с иными видами характеристик преступлений, речь о которых ведется в других юридических науках [1, с. 101]. Особенно это заметно при сопоставлении с криминалистической характеристикой преступления. Данное обстоятельство побуждает некоторых исследователей говорить о том, что оперативно-разыскная характеристика преступлений – это новый фантом ОРД, а следовательно, ее дальнейшая разработка научной значимости не имеет [2, с. 94]. На наш взгляд, эта точка зрения неверна и не может быть принята в качестве верной ни при каких обстоятельствах. Как отметил В.Ф. Луговик, «теория оперативно-розыскной деятельности на протяжении своего развития и совершенствования выработала свое понятие характеристики преступлений, которое получило название оперативно-розыскной» [3, с. 13-16].

Признавая схожесть оперативно-разыскной характеристики преступлений с иными видами их характеристик, В.Д. Ларичев тем не менее отмечает, что «главной целью оперативно-розыскной характеристики преступлений является предоставление сотрудникам уголовного розыска и иным субъектам оперативно-розыскной деятельности наглядного представления о том, какие могут быть проведены оперативно-розыскные мероприятия, для чего и каким образом» [4, с. 15]. Именно через цель конструирования всех признаков оперативно-разыскной характеристики преступлений необходимо определять детерминантную сущность ее использования. Ни одна другая характеристика преступлений не может дать возможность субъекту ОРД спланировать и организовать оперативно-разыскные мероприятия (далее – ОРМ), проводимые как гласно, так и негласно, которые в конечном итоге позволят раскрыть преступление. Поэтому оперативно-разыскную характеристику преступления как элемент оперативно-разыскной, поисковой и противоборствующей преступлениям деятельности субъектов ОРД следует считать важнейшей самостоятельной категорией, требующей самого тщательного подхода к ее изучению. В связи с этим считаем необходимым рассмотреть основные элементы оперативно-разыскной характеристики IT-преступлений.

Учитывая вышеизложенное, можем предположить, что в единую систему признаков оперативно-разыскной характеристики преступлений исследуемого нами вида входят следующие элементы:

- современное состояние преступности в сфере ИТТ;
- обстановка совершения преступления;

- оперативно значимые данные о личности киберпреступника и потерпевших;
- способы совершения преступления;
- оперативно-разыскная профилактика.

О современном состоянии преступности в сфере ИТТ и актуальности вопросов противодействия ей свидетельствуют сведения статистики. Так, по данным Главного информационно-аналитического центра МВД России, за последние годы был зарегистрирован существенный рост количества IT-преступлений (см. таблицу 1)[1].

Исходя из результатов анализа приведенных статистических сведений о количестве зарегистрированных IT-преступлений, можно сделать следующие выводы:

- борьба с IT-преступлениями остается актуальной проблемой;
- почти половина таких преступлений относится к категориям тяжких и особо тяжких;
- значительное количество преступлений данного вида совершены с использованием сети Интернет, а также мобильных средств связи.

Волгоградская область не является исключением, здесь также наблюдается расширение масштабов преступности в сфере ИТТ, что влечет за собой рост размеров причиняемого материального ущерба. Согласно статистике Информационного центра ГУ МВД России по Волгоградской области, в регионе наблюдается увеличение количества IT-преступлений (см. таблицу 2)[2].

В целях противодействия угрозам, генерируемым киберпреступностью, коллегия МВД России в конце 2019 года приняла решение о проведении организационно-штатных мероприятий, направленных на создание в подразделениях по контролю за оборотом наркотиков (ГУКОН МВД России), по противодействию экстремизму (ГУПЭ МВД России), уголовного розыска (ГУУР МВД России), экономической безопасности и противодействия коррупции (ГУЭПиПК МВД России), следственных подразделениях (СД МВД России), подразделениях дознания (УОД МВД России), специальных технических мероприятий (БСТМ МВД России) отделов, отделений, групп, специализирующихся на противодействии IT-преступлениям[3].

Анализ складывающейся оперативной обстановки свидетельствует, что, несмотря на предпринимаемые государством меры по предотвращению развития негативной динамики показателей преступности в сфере ИТТ, они оказываются недостаточно эффективными и требуют скорейшего расширения. В связи с этим в сентябре 2022 года в системе МВД России создано Управление по организации борьбы с противоправным использованием информационно-коммуникационных технологий (далее – УБК МВД России)[4]. В рамках нашего исследования, как очевидно, необходимо рассмотреть специфику деятельности этого нового оперативного подразделения органов внутренних дел. Следует уделить внимание наиболее значимым направлениям его работы, связанным в первую очередь с документированием и раскрытием преступлений изучаемого нами вида. Мы сделаем это на примере Волгоградской области.

Прежде всего подчеркнем, что данное оперативное подразделение осуществляет ОРД в полном объеме[5]. Отдел по борьбе с противоправным использованием информационно-телекоммуникационных технологий (далее – ОБК ГУ МВД России по Волгоградской области) был образован 1 февраля 2023 года, а фактически осуществлять ОРД его сотрудники стали с ноября 2023 года. Основными задачами ОБК ГУ МВД России по Волгоградской области являются выявление, предупреждение, пресечение и раскрытие тяжких и особо тяжких преступлений:

- против жизни и здоровья, половой неприкосновенности и половой свободы личности, связанных с использованием и распространением запрещенной информации в информационно-телекоммуникационных сетях, включая сеть Интернет;
- сопряженных с нарушением неприкосновенности частной жизни, тайны переписки и сообщений, передаваемых по сетям электрической связи, посредством неправомерного доступа к компьютерной информации и (или) использования вредоносного программного обеспечения;
- против собственности и в сфере экономической деятельности, совершенных по совокупности с неправомерным доступом к компьютерной информации и (или) использованием вредоносного программного обеспечения;
- направленных на неправомерный доступ к компьютерной информации;
- связанных с созданием, использованием и распространением вредоносных компьютерных программ, нарушением правил эксплуатации информационно-телекоммуникационных сетей и средств хранения, обработки или передачи компьютерной информации;
- касающихся нарушений авторских и смежных прав, совершенных по совокупности с неправомерным доступом к компьютерной информации и (или) использованием вредоносного программного обеспечения;

[1] Представлена информация о состоянии преступности в России за 2021-2023 годы с официального сайта МВД России.
[2] Комплексный анализ состояния преступности и основных результатов оперативно-служебной деятельности органов и подразделений ГУ МВД России по Волгоградской области за 2023 г. // Архив ГУ МВД России по Волгоградской области.
[3] См.: п. 23 Приказа МВД России от 25.11.2019 № 878 «Об объявлении решения коллегии Министерства внутренних дел Российской Федерации от 1 ноября 2019 г. № 3км».
[4] Указ Президента Российской Федерации от 30.09.2022 № 688 «О внесении изменений в некоторые акты Президента Российской Федерации»; приказ МВД России от 11.10.2022 № 747 «О создании Управления по организации борьбы с противоправным использованием информационно-коммуникационных технологий Министерства внутренних дел Российской Федерации».
[5] Приказ МВД России от 31.03.2023 № 199 «Об утверждении Перечня оперативных подразделений органов внутренних дел Российской Федерации, правомочных осуществлять оперативно-розыскную деятельность».

- совершенных в рамках деятельности транснациональных, межрегиональных организованных групп и преступных сообществ (преступных организаций) с использованием (в сфере) информационно-коммуникационных технологий[1].

Таким образом, МВД России были предприняты меры организационно-правового характера, направленные, в частности, на определение полномочий оперативных подразделений органов внутренних дел, осуществляющих противодействие преступности в сфере ИТТ[2].

МЕТОДЫ

При проведении исследования применялся общенаучный диалектический метод познания окружающей действительности, предполагающий полное и всестороннее изучение явлений, рассмотрение связей и противоречий между ними. Кроме того, были использованы: метод описания, необходимый для сбора фактического материала о проблемах, возникающих в процессе противодействия IT-преступлениям; метод логического осмысления, позволивший определить понятие «оперативно-разыскной характеристики преступлений» и его элементы; абстрагирование и обобщение, призванные систематизировать установленные факты и дать им толкование. Проведен анализ статистических данных, характеризующих современное состояние противодействия преступности в сфере ИТТ, а также личность киберпреступников.

РЕЗУЛЬТАТЫ

С учетом задач нашего исследования необходимо проанализировать эффективность работы подразделений УБК МВД России, осуществляющих борьбу с IT-преступлениями, способы совершения таких преступлений, а также факторы, влияющие на динамику преступности рассматриваемого вида. При этом рассмотрим наиболее значимые, на наш взгляд, направления деятельности данного оперативного подразделения, связанные с документированием и раскрытием IT-преступлений, на примере Волгоградской области.

Преступления против личности, в частности против половой неприкосновенности и половой свободы несовершеннолетних, связанные с использованием и распространением запрещенной информации в информационно-телекоммуникационных сетях, включая сеть Интернет (п. «д» ч. 2 ст. 110, п. «д» ч. 3, ч. 4-6 ст. 110.1, ч. 2 ст. 110.2, ч. 2 ст. 128.1, п. «б» ч. 4 ст. 132, п. «б» ч. 3 ст. 133, ст. 135 УК РФ).

Несовершеннолетние – это лица, которые обоснованно считаются наиболее уязвимыми и незащищенными. Это связано с тем, что дети еще не обладают полной дееспособностью и в силу возраста не могут самостоятельно защитить свои права и законные интересы. По этой причине они становятся жертвами преступлений со стороны взрослых, подвергаясь насилию, совершенному бесконтактным способом посредством современных коммуникационных технологий, включая сеть Интернет [5, с. 30]. Преступления рассматриваемого вида совершаются посредством социальных сетей, электронной почты, мобильных приложений «WhatsApp» и «Viber», интернет-сайтов знакомств, форумов, чатов и т.п. В ходе доказывания вины киберпреступника перед сотрудниками ОБК ГУ МВД России по Волгоградской области прежде всего стоит задача документирования его переписки с несовершеннолетним, не достигшим возраста шестнадцати лет. Кроме того, необходимо подтвердить факт использования аккаунта в социальных сетях для осуществления противоправной деятельности именно этим преступником, а не кем-то другим. Данные задачи решаются путем проведения компьютерной экспертизы, а также получения информации от владельцев социальных сетей и мессенджеров [6, с. 76].

В качестве примера эффективной работы по выявлению и документированию подобных преступлений рассмотрим реализацию материалов ОРД сотрудниками ОБК ГУ МВД России по Волгоградской области в отношении жителя г. Волгограда ранее не судимого К. В период с августа по октябрь 2023 года в ходе проведения комплекса оперативно-разыскных мероприятий было установлено, что фигурант, находясь по месту своего проживания, используя мобильный телефон с выходом в информационно-телекоммуникационную сеть Интернет и страницу в социальной сети «ВКонтакте, с целью удовлетворения своих половых потребностей осуществлял переписку с пятью заведомо для него несовершеннолетними лицами мужского пола, совершая тем самым развратные действия без применения насилия. По данному факту следственным отделом по Тракторозаводскому району г. Волгоград СУ СК России по Волгоградской области 25 сентября 2023 года возбуждено уголовное дело по признакам преступления, предусмотренного ч. 3 ст. 135 УК РФ, а в отношении К. вынесено постановление о привлечении в качестве обвиняемого. К. свою вину в совершенных преступлениях признал полностью и дал признательные показания, после чего был задержан в порядке ст. 91 УПК РФ.

Преступления против собственности и в сфере экономической деятельности (ст.ст. 158, 159, 159.3, 159.6, 163, 165 УК РФ (кроме ст. 159.6 УК РФ) в совокупности со ст. 272, 273 УК РФ). При анализе таких преступлений, деятельность по выявлению и раскрытию которых входит в компетенцию ОБК

[1] Приказ ГУ МВД России по Волгоградской области от 30.03.2023 № 176 «Об утверждении Положения об отделе по борьбе с противоправным использованием информационно-коммуникационных технологий ГУ МВД России по Волгоградской области».

[2] Приказ МВД России от 05.04.2022 № 236 «Об определении полномочий оперативных подразделений органов внутренних дел Российской Федерации по противодействию преступлениям, совершенным с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации»; приказ МВД России от 27.07.2023 № 547 «О внесении изменений в приказ МВД России от 5 апреля 2022 г. № 236 «Об определении полномочий оперативных подразделений органов внутренних дел Российской Федерации по противодействию преступлениям, совершенным с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации».

ГУ МВД России по Волгоградской области, следует учитывать, что в данном случае все преступные деяния (за исключением тех, ответственность за совершение которых предусмотрена ст. 159.6 УК РФ) требуют дополнительной квалификации по ст. 272 и/или ст. 273 УК РФ. Это обусловлено тем, что злоумышленники в процессе совершения IT-преступлений осуществляют неправомерный доступ к компьютерной информации и (или) создают, используют, распространяют вредоносные компьютерные программы, способные удалять, блокировать, модифицировать компьютерную информацию либо иным образом вмешиваться в работу средств хранения, обработки, передачи компьютерной информации или информационно-телекоммуникационных сетей.

Заведомо ложное сообщение об акте терроризма (ст. 207 УК РФ).

Киберпреступники, пользуясь тем, что их потенциальные жертвы (чаще всего это несовершеннолетние и граждане пенсионного возраста) не соблюдают правил информационной безопасности и размещают в свободном доступе данные о себе и своих родственниках в социальных сетях, мессенджерах, аккаунтах компьютерных игр, собирают сведения о них, а затем осуществляют массовые рассылки сообщений о террористических атаках от их лица. Это может стать причиной негативных последствий в виде проведения правоохранительными органами процессуальных проверок в порядке ст.ст. 144-145 УПК РФ. Описанные противоправные деяния создают предпосылки к дестабилизации оперативной обстановки в регионе и стране в целом.

Преступления в сфере компьютерной информации (ст.ст. 272, 273, 274, 274.1 гл. 28 УК РФ).

Согласно статистике за 2023 г., опубликованной «Лабораторией Касперского», злоумышленники постоянно модернизируют свой арсенал вредоносного программного обеспечения, позволяющего им преодолевать не отвечающие современным требованиям средства защиты информации, хранящейся на компьютерах, и способов его распространения. Количество ежедневно появляющихся новых вредоносных программ доходит до 411 тысяч[1]. Кроме того, предметом IT-преступлений является и оборудование, обеспечивающее информационно-телекоммуникационные процессы. Причем необходимо иметь в виду, что возможности Интернета активно используют представители спецслужб иностранных государств для дестабилизации общественно-политической обстановки (например для организации акций неповиновения законным властям и других противоправных действий).

С учетом вышеизложенного считаем, что все IT-преступления можно условно разделить на две группы:

1) связанные с вмешательством в работу компьютеров;

2) совершаемые с использованием компьютера.

IT-преступления, связанные с вмешательством в работу компьютеров.

1. Неправомерный доступ к компьютерной информации.

Это деяние, которое включает в себя незаконное получение доступа к компьютерной информации без разрешения владельца или пользователя этой информации, образующее состав преступления.

2. Разработка и распространение компьютерных вирусов.

Компьютерные вирусы были и остаются одной из наиболее распространенных причин утраты информации. Известны случаи, когда они блокировали работу организаций и предприятий. Так, 25 января 2003 года компьютерный червь «Slammer» обрушил корпоративную сеть атомной электростанции в штате Огайо (США), после чего распространился на системы мониторинга безопасности и охлаждения АЭС. В сентябре 2010 года в Иране около 30 тысяч компьютерных систем промышленных объектов были заражены вирусом «Stuxnet». Взлом привел к остановке работы более 1300 центрифуг по обогащению урана на объекте в Натанзеи и переносу сроков запуска АЭС «Бушер»[2]. 27 июня 2017 года вирус-вымогатель заблокировал компьютеры радиационного мониторинга Чернобыльской АЭС[3].

Компьютерный вирус – это программа, которая может копировать себя и распространяться без ведома пользователя, часто нанося вред компьютеру или хранящийся на нем информации. Вирусы создаются для различных целей, в том числе для кражи персональных данных, повреждения файлов, нарушения работы компьютера или даже его использования для атаки на другие компьютеры. Основными каналами распространения вирусов являются: электронная почта, интернет-сайты, съемные носители информации и др.

С целью обеспечения информационной безопасности необходимо использовать антивирусные программы, быть осторожным при открытии электронных писем или загрузке файлов из ненадежных источников, чтобы предотвратить заражение компьютера вирусом.

3. Ввод в компьютер пользователя вредоносных программ.

В данном случае вредоносное программное обеспечение (например вирусы, трояны, шпионское ПО и т.д.) вводится в компьютер или компьютерную систему без ведома пользователя. Это может произойти различными способами. К числу основных из них относятся: загрузка вредоносного программного обеспечения из Интернета при посещении неизвестных сайтов или при загрузке

[1] Решения «Лаборатории Касперского» ежедневно находят 411 тыс. вредоносных файлов // Лаборатория Касперского: сайт // URL: https://safe.cnews.ru/news/line/2023-12-04_resheniya_laboratorii_kasperskogo (дата обращения: 01.05.2024).

[2] Кибератаки на ядерные объекты // Коммерсант: сайт // URL: https://www.kommersant.ru/doc/3196397 (дата обращения: 01.05.2024).

[3] Вирус-вымогатель Petya поразил Чернобыльскую АЭС // РИА «Новости»: сайт // URL: https://ria.ru/20170627/1497397238.html (дата обращения: 01.05.2024).

файлов из ненадежных источников; открытие в электронной почте писем с вложениями, которые при просмотре автоматически устанавливают вредоносное программное обеспечение на компьютер; установка вредоносных программ посредством съемных носителей информации, таких как USB-флешки или CD/DVD-диски, на которых находятся компьютерные вирусы; установка вредоносного программного обеспечения через уязвимости в операционной системе компьютера или используемых на нем приложений (например в процессе автоматической установки обновлений операционной системы, браузеров, драйверов и т.д.); установка вредоносного приложения в результате принуждения пользователя посредством техник социальной инженерии (например, когда его вводят в заблуждение, требуя при этом установить программное обеспечение через фишинговые электронные письма или поддельные сайты).

4. Неправомерное нарушение порядка эксплуатации компьютера, систем компьютеров или их сетей либо умышленное нарушение установленных правил и процедур.

Это действия, которые могут привести к сбоям в работе компьютеров и их компьютерных систем, потере данных или другим негативным последствиям (например взлом систем, использование вредоносного программного обеспечения, несанкционированный доступ к конфиденциальной информации и т.п.).

5. Хищение компьютерной информации.

Следует заметить, что доказать совершение такого преступления, как хищение компьютерной информации, согласно нормам действующего УК РФ, достаточно проблематично [7, с. 26]. Похищенная компьютерная информация не обязательно удаляется, ее можно просто скопировать. При этом законному владельцу наносится значительный вред, связанный, например, с лишением конкурентного преимущества или распространением информации ограниченного доступа.

6. Уничтожение компьютерной информации.

Прежде всего это процесс, при котором информация, хранящаяся на компьютере или в компьютерной системе, намеренно удаляется или становится недоступной. Добиться преступного результата в данном случае можно различными способами: удаление файлов с компьютера; повреждение файлов, что приводит к их недоступности; форматирование диска, в результате чего удаляется вся хранившаяся на нем информация; уничтожение данных на компьютере, например, путем перезаписи файлов или удаления их из файловой таблицы; уничтожение данных на компьютере или в компьютерной системе посредством проведения кибератаки.

7. Подделка компьютерной информации.

Это действия, в результате которых информация, хранящаяся на компьютере либо в компьютерной системе, намеренно изменяется или фальсифицируется без ведома или согласия ее владельца. Данный способ совершения IT-преступления используется, как правило, для изменения конечной информации, запрашиваемой заказчиком (например результатов какого-либо конкурса и т.п.).

IT-преступления, совершаемые с использованием компьютера.

Анализ второй группы преступлений рассматриваемого нами вида позволяет сделать вывод о том, что в качестве средств их совершения используется переносные (портативные) компьютеры – ноутбуки, планшеты, смартфоны. Правоприменительная практика свидетельствует, что данные устройства способны хранить, передавать и обрабатывать информацию, которая необходима для различных противоправных действий [8, с. 145]. Поэтому компьютерную технику следует рассматривать в качестве элемента оперативно-разыскной характеристики IT-преступлений. В этом контексте она требует особого внимания со стороны оперативных сотрудников ОБК ГУ МВД России по Волгоградской области. Это необходимо для получения доказательной информации и обеспечения надлежащих условий для уголовного судопроизводства.

Обстановка совершения преступления как элемент оперативно-разыскной характеристики IT-преступлений дает ответы на такие вопросы, как «где и когда совершаются эти преступления». При этом, конечно, полностью унифицировать ответы на подобные вопросы невозможно, так как каждый случай совершения преступления по-своему уникален, и, по сути, IT-преступление может совершаться в любом месте и в любое время.

Следующим по значимости элементом оперативно-разыскной характеристики IT-преступлений является личность киберпреступника. Исследователи в области криминалистики, криминологии, уголовного права, оперативно-разыскной деятельности, психологии и других наук для более эффективного анализа и предотвращения преступлений разделяют преступников на группы по различным признакам (например пол, возраст, профессия, образование и т.д.). Рассмотрим некоторые из них:

- лица (профессиональные киберпреступники), которые используют свои технические и интеллектуальные способности в области ИТТ в качестве специального инструмента для достижения противоправных целей;

- лица, не являющиеся специалистами в сфере ИТТ, но тесно связанные с киберпреступниками через свои профессиональные контакты или личные отношения (например сотрудники банков или коммерческих компаний, которые имеют доступ к конфиденциальной информации);

- лица, не имеющие специального образования, но обладающие определенными навыками в области ИТТ (позволяющими, например, создавать простые вредоносные программы или использовать готовые для совершения IT-преступлений).

Кроме того, необходимо учитывать, что киберпреступления могут совершаться единолично, организованными группами специалистов в области ИТТ, транснациональными преступными группами со сложной иерархической структурой. Такие группы используют методы противодействия правоохранительным органам, позволяющие уходить

из поля зрения оперативников [9, с. 59]. В качестве инструмента такого противодействия киберпреступники используют средства анонимизации в сети, которые называются VPN (виртуальная частная сеть). Смысл VPN заключается в том, что пользователь Интернета, перед тем как войти на сайт, подключается к серверу третьего лица, как правило, находящегося на территории иного государства, обычно недружественного. VPN может скрывать реальный IP-адрес пользователя. Одним из самых надежных способов противодействия правоохранительным органам и легализации доходов от преступной деятельности, используемых киберпреступниками, является перевод денежных средств из официальных платежных систем в различные криптовалюты – «биткоин» и т.п. [10, с. 119]. При этом ими неоднократно осуществляется перевод криптовалюты с одного анонимного электронного счета на другой, именуемый в преступной среде «битмиксер». Фактически он представляет собой сервисы (сайты), разбивающие перевод на множество частей и смешивающие эти части с «монетами» (денежными средствами) других пользователей. Таким образом, киберпреступники скрывают поступление денежных средств и их последующий перевод до конечной точки обналичивания, которой в большинстве случаев является так называемая «дроп-карта». На сленге киберпреступников «дропом» (от англ. drop – сбрасывать) называют подставное лицо, на которое оформлены банковские карты, используемые для обналичивания.

Анализируя оперативно значимые данные о личности, нельзя обойти вниманием тот факт, что киберпреступниками являются лица разных возрастных групп. Некоторые из них – это молодые люди, которые только начинают осваивать компьютерные технологии (и даже подростки, которые имеют особые навыки и технические возможности для совершения разного рода IT-преступлений) [11, с. 8], другие – опытные хакеры и программисты в возрасте от 16 до 35 лет. При этом примерно в 90% случаев киберпреступником является мужчина, в 95% случаев – ранее не судимый [12, с. 151]. Знание этих признаков способствует эффективной организации работы по предупреждению и раскрытию преступлений рассматриваемого нами вида.

Необходимо отметить, что, помимо мероприятий, направленных на выявление и раскрытие IT-преступлений, на подразделения ОБК ГУ МВД России по Волгоградской области возложены задачи по осуществлению их профилактики. Она также является элементом оперативно-разыскной характеристики таких преступлений. Представим ряд положительных примеров проводимой на территории Волгоградской области профилактической работы такого рода:

1. Оперативно-профилактическое мероприятие «Сорняк» организуется в целях выявления, предупреждения, пресечения преступлений и административных правонарушений, связанных с эксплуатацией женщин и детей, а также производством и распространением с использованием информационных технологий порнографической продукции.

2. До сведения граждан доводится информация, направленная на повышение уровня их цифровой грамотности. Считаем, что это одна из важнейших задач органов внутренних дел. Ее сформулировал Президент В.В. Путин в 2023 году на заседании коллегии МВД России. Под грамотностью следует понимать не только владение навыками пользования компьютерной техникой, но и знание правил «гигиены» в Интернете, умение обнаруживать угрозы на ранней стадии. Как представляется, даже минимальный объем знаний о наиболее распространенных видах кибератак может способствовать предотвращению совершения IT-преступления в отношении лица, обладающего такими знаниями.

3. Разрабатываются и распространяются методические рекомендации и алгоритмы действий, содержащих, кроме прочего, сведения о мерах профилактического характера. Эта деятельность осуществляется, в частности, с целью организации незамедлительного информирования ОБК ГУ МВД России по Волгоградской области руководителями территориальных органов внутренних дел региона о фактах выявления преступлений, например, против несовершеннолетних, совершенных с использованием ИТТ[1].

4. Участие в деятельности рабочей группы, созданной на базе Отделения «Волгоград» Южного главного управления ЦБ РФ, в состав которой входят сотрудники правоохранительных органов, в том числе прокуратуры, представители кредитно-финансовых организаций, компаний сотовой связи и другие заинтересованные субъекты, направленной на выработку и реализацию на региональном уровне мер по предупреждению киберпреступлений.

ЗАКЛЮЧЕНИЕ

В настоящее время на существующее около двух лет УБК МВД России и региональные подразделения по организации борьбы с противоправным использованием информационно-коммуникационных технологий государством возложены задачи по обеспечению безопасности в киберпространстве. На наш взгляд, эффективность этой деятельности будет зависеть от нескольких ключевых факторов:

1. Необходимо совершенствовать действующее уголовное законодательство. Так, например, невозможно привлечь лицо к уголовной ответственности за нелегальный майнинг и DDoS-атаку, если это не повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации, а просто исчерпывает ресурсы чужого устройства или делает невозможным использование какого-либо интернет-сервиса [13, с. 32].

За изменение идентификационного кода абонентского устройства сотовой связи, создание дубликата SIM-карты идентификации абонента сотовой связи уголовная ответственность не предусмотрена. Вместе с тем, используя только або-

[1] Методические рекомендации ОБК ГУ МВД России по Волгоградской области от 07.03.2024 № 6/1341 // Архив ОБК ГУ МВД России по Волгоградской области.

нентский номер, субъекты ОРД могут установить личность абонента, а также другую информацию, представляющую оперативный интерес [14, с. 124]. В то же время в Уголовном кодексе Республики Казахстана норма, позволяющая привлечь лицо к уголовной ответственности за вышеуказанные действия, закреплена.

Еще в 2013 году были внесены изменения в Федеральный закон от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности», которые в один ряд с экологической, государственной, экономической безопасностью Российской Федерации поставили информационную безопасность и тем самым дали возможность проведения оперативно-разыскных мероприятий в сфере противодействия киберпреступности всем заинтересованным субъектам, правомочным осуществлять ОРД[1]. Однако, к сожалению, следует признать, что это не является прямым указанием на возможность проведения оперативно-разыскных мероприятий в сети Интернет. Законодатель в ст. 10 Федерального закона «Об оперативно-розыскной деятельности» закрепляет лишь возможность создания и использования информационных систем, без какой-либо конкретизации. В связи с этим предлагаем дополнить эту статью следующим текстом:

«Органы, осуществляющие оперативно-розыскную деятельность, для решения задач, возложенных на них настоящим Федеральным законом, могут создавать и использовать информационные системы, *включая специальные программы, обеспечивающие удаленный доступ к устройствам посредством информационно-телекоммуникационной сети Интернет*, а также заводить дела оперативного учета».

Отметим внимание на то, что подобного рода практика апробирована и с успехом применяется в странах Европы и США с 2010 года [15, с. 19]. Правоохранительными органами используются программы-помощники – «правоохранительные трояны», – которые позволяют в целях раскрытия и расследования преступлений получать доступ к устройству лица, совершившего, совершающего или готовящего совершение IT-преступлений. В отечественной правоохранительной системе такие программы не используются, специально для нее они не разрабатываются, так как их статус в правовом поле не определен. Хотя такое программное обеспечение существует. Так, например, удаленный доступ к электронным устройствам физических и юридических лиц обеспечивают зарубежные программы «TeamViewer» (бесплатный удаленный контроль с устройств, работающих на базе операционной системы «Android» или «Windows» и др.).

2. Необходимо укрепить взаимодействие между российскими и зарубежными правоохранительными органами. Международная практика по предотвращению, выявлению и расследованию IT-преступлений ограничивается руководящими принципами и рекомендуемыми стандартами сотрудничества между субъектами информационной безопасности на семинарах, конференциях, проводимых на площадках ООН и других организаций, в которых состоит Российская Федерация [16, с. 150]. Подчеркнем, что в настоящее время сотрудничество правоохранительных органов России в сфере ИТТ в условиях беспрецедентного санкционного давления со стороны США и их союзников возможно только с официальными представителями дружественных стран.

3. Необходимо повысить потенциал специалистов, занимающихся выявлением и расследованием киберпреступлений. Следует согласиться с мнением Д.А. Синькова, который отмечал, что «в настоящее время этой работой занимается до 70% специалистов, которые слабо разбираются в специфике распространения компьютерной информации. Это недопустимо для эффективной работы специальных подразделений в сфере обеспечения компьютерной безопасности» [17]. На эту проблему указали и опрошенные нами респонденты из числа сотрудников оперативных подразделений ГУ МВД России по Волгоградской области, осуществляющих противодействие IT-преступлениям. Считаем, что у МВД России существует острая потребность в подготовке высококвалифицированных кадров, способных эффективно выявлять, раскрывать и расследовать киберпреступления.

Учет в работе по противодействию IT-преступности перечисленных нами факторов будет способствовать решению задач по обеспечению безопасности в киберпространстве и повышению степени защищенности граждан России от кибератак. ■

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Катков С.В., Белокобыльская О.И., Горных С.А. Оперативно-розыскная характеристика преступлений, совершаемых в кредитно-финансовой сфере: отдельные вопросы теории и практики // Вестник Волгоградской академии МВД России. 2019. № 2 (49). С. 100-110.

2. Захарцев С.И., Кирюшкина Н.О. Новые фантомы оперативно-розыскной деятельности: оперативно-розыскная характеристика и оперативно-розыскной кодекс // Юридическая наука: история и современность. 2013. № 9. С. 94-101.

3. Луговик В.Ф. Проблемы формирования учения об оперативно-розыскной характеристике преступлений // Оперативник (сыщик). 2006. № 4 (9). С. 13-16.

4. Ларичев В.Д. Оперативно-розыскная характеристика экономических преступлений: понятие и содержание // Оперативник (сыщик). 2009. № 1 (18). С. 11-16.

5. Алексеева А.П., Ничуговская О.Н. Киберпреступность: основные черты и формы проявления // Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений. 2017. № 1. С. 27-34.

[1] Федеральный закон от 21.12.2013 № 369-ФЗ «О внесении изменений в Федеральный закон «Об оперативно-розыскной деятельности» и статью 13 Федерального закона «О федеральной службе безопасности»».

6. Алексеева А.П. Киберпреступность: насколько реальна угроза // Научно-методический электронный журнал «Концепт». 2017. Т. 31. С. 76-80.

7. Алексеева А.П. Перспективы развития уголовного законодательства в киберсфере // Подготовка сотрудников полиции к использованию информационных технологий в борьбе с преступностью: сборник научных трудов по материалам II Всероссийской межвузовской научно-практической конференции. Волгоград, 6 декабря 2016 г. Вып. 2. Волгоград: ВА МВД России, 2017. С. 24-31.

8. Шахматов А.В., Бажуков В.Б. Оперативно-розыскное исследование электронных носителей информации при выявлении и раскрытии преступлений в кредитно-банковской сфере // Вестник Санкт-Петербургского университета МВД России. 2014. № 2 (62). С. 143-147.

9. Кушниренко С.П. Характеристика субъекта как элемента системы преступного посягательства в сфере высоких технологий // Вестник Санкт-Петербургского университета МВД России. 2005. № 4 (28-2). С. 52-60.

10. Карпов Н.О. Предмет неправомерного оборота средств платежей (правовой и криминалистический аспекты) // Вестник Санкт-Петербургского университета МВД России. 2017. № 3 (75). С. 119-122.

11. Глазатова С.В., Бурцева Е.В., Медведева С.В. Киберпреступления, совершаемые несовершеннолетними: проблемы расследования // Российский следователь. 2021. № 2. С. 7-10.

12. Жижина М.В., Завьялова Д.В. Личность субъекта преступлений в сфере компьютерной информации как системообразующий элемент криминалистической характеристики (по материалам российских и зарубежных источников) // Актуальные проблемы российского права. 2022. № 5. С. 149-158.

13. Алексеева А.П., Лахин А.Н. Законодательные инициативы в сфере ужесточения наказания за хищение денег с банковских счетов или счетов в электронных платежных системах // Актуальные проблемы уголовного законодательства на современном этапе: сборник научных трудов Международной научно-практической конференции. Волгоград, 18-19 мая 2017 г. Волгоград: ВА МВД России, 2017. С. 30-34.

14. Катков С.В., Семененко Г.М., Костенко Н.С., Алексеева А.П. О мерах совершенствования организации работы оперативных и следственных подразделений МВД России по выявлению, раскрытию и расследованию хищений денежных средств с использованием банковских карт на территории Российской Федерации // Вестник Волгоградской академии МВД России. 2020. № 4 (55). С. 123-128.

15. Харевич Д.Л. Негласное расследование в Германии: Монография. Минск: Академия МВД Республики Беларусь, 2010. 287 с.

16. Ростов К.Т., Игнатенко Д.И., Бондуровский В.В., Бухаров Н.Н. Новые информационные технологии в практике работы правоохранительных органов // Вестник Санкт-Петербургского университета МВД России. 1999. № 1 (1). С. 143-153.

17. Синьков Д.А. Повышение эффективности расследования преступлений в сфере компьютерной информации // Современные научные исследования и инновации. 2017. № 8. С. 17.

REFERENCES

1. Katkov S.V., Belokobyl'skaya O.I., Gornykh S.A. Operativno-rozysknaya kharakteristika prestupleniy, sovershayemykh v kreditno-finansovoy sfere: otdel'nyye voprosy teorii i praktiki // Vestnik Volgogradskoy akademii MVD Rossii. 2019. № 2 (49). S. 100-110.

2. Zakhartsev S.I., Kiryushkina N.O. Novyye fantomy operativno-rozysknoy deyatel'nosti: operativno-rozysknaya kharakteristika i operativno-rozysknoy kodeks // Yuridicheskaya nauka: istoriya i sovremennost'. 2013. № 9. S. 94-101.

3. Lugovik V.F. Problemy formirovaniya ucheniya ob operativno-rozysknoy kharakteristike prestupleniy // Operativnik (syshchik). 2006. № 4 (9). S. 13-16.

4. Larichev V.D. Operativno-rozysknaya kharakteristika ekonomicheskikh prestupleniy: ponyatiye i soderzhaniye // Operativnik (syshchik). 2009. № 1 (18). S. 11-16.

5. Alekseyeva A.P., Nichugovskaya O.N. Kiberprestupnost': osnovnyye cherty i formy proyavleniya // Prestupnost' v sfere informatsionnykh i telekommunikatsionnykh tekhnologiy: problemy preduprezhdeniya, raskrytiya i rassledovaniya prestupleniy. 2017. № 1. S. 27-34.

6. Alekseyeva A.P. Kiberprestupnost': naskol'ko real'na ugroza // Nauchno-metodicheskiy elektronnyy zhurnal «Kontsept». 2017. T. 31. S. 76-80.

7. Alekseyeva A.P. Perspektivy razvitiya ugolovnogo zakonodatel'stva v kibersfere // Podgotovka sotrudnikov politsii k ispol'zovaniyu informatsionnykh tekhnologiy v bor'be s prestupnost'yu: sbornik nauchnykh trudov po materialam II Vserossiyskoy mezhvuzovskoy nauchno-prakticheskoy konferentsii. Volgograd, 6 dekabrya 2016 g. Vyp. 2. Volgograd: VA MVD Rossii, 2017. S. 24-31.

8. Shakhmatov A.V., Bazhukov V.B. Operativno-rozysknoye issledovaniye elektronnykh nositeley informatsii pri vyyavlenii i raskrytii prestupleniy v kreditno-bankovskoy sfere // Vestnik Sankt-Peterburgskogo universiteta MVD Rossii. 2014. № 2 (62). S. 143-147.

9. Kushnirenko S.P. Kharakteristika sub»yekta kak elementa sistemy prestupnogo posyagatel'stva v sfere vysokikh tekhnologiy // Vestnik Sankt-Peterburgskogo universiteta MVD Rossii. 2005. № 4 (28-2). S. 52-60.

10. Karpov N.O. Predmet nepravomernogo oborota sredstv platezhey (pravovoy i kriminalisticheskiy aspekty) // Vestnik Sankt-Peterburgskogo universiteta MVD Rossii. 2017. № 3 (75). S. 119-122.
11. Glazatova S.V., Burtseva Ye.V., Medvedeva S.V. Kiberprestupleniya, sovershayemyye nesovershennoletnimi: problemy rassledovaniya // Rossiyskiy sledovatel'. 2021. № 2. S. 7-10.
12. Zhizhina M.V., Zav'yalova D.V. Lichnost' sub»yekta prestupleniy v sfere komp'yuternoy informatsii kak sistemoobrazuyushchiy element kriminalisticheskoy kharakteristiki (po materialam rossiyskikh i zarubezhnykh istochnikov) // Aktual'nyye problemy rossiyskogo prava. 2022. № 5. S. 149-158.
13. Alekseyeva A.P., Lakhin A.N. Zakonodatel'nyye initsiativy v sfere uzhestocheniya nakazaniya za khishcheniye deneg s bankovskikh schetov ili schetov v elektronnykh platezhnykh sistemakh // Aktual'nyye problemy ugolovnogo zakonodatel'stva na sovremennom etape: sbornik nauchnykh trudov Mezhdunarodnoy nauchno-prakticheskoy konferentsii. Volgograd, 18-19 maya 2017 g. Volgograd: VA MVD Rossii, 2017. S. 30-34.
14. Katkov S.V., Semenenko G.M., Kostenko N.S., Alekseyeva A.P. O merakh sovershenstvovaniya organizatsii raboty operativnykh i sledstvennykh podrazdeleniy MVD Rossii po vyyavleniyu, raskrytiyu i rassledovaniyu khishcheniy denezhnykh sredstv s ispol'zovaniyem bankovskikh kart na territorii Rossiyskoy Federatsii // Vestnik Volgogradskoy akademii MVD Rossii. 2020. № 4 (55). S. 123-128.
15. Kharevich D.L. Neglasnoye rassledovaniye v Germanii: Monografiya. Minsk: Akademiya MVD Respubliki Belarus', 2010. 287 s.
16. Rostov K.T., Ignatenko D.I., Bondurovskiy V.V., Bukharov N.N. Novyye informatsionnyye tekhnologii v praktike raboty pravookhranitel'nykh organov // Vestnik Sankt-Peterburgskogo universiteta MVD Rossii. 1999. № 1 (1). S. 143-153.
17. Sin'kov D.A. Povysheniye effektivnosti rassledovaniya prestupleniy v sfere komp'yuternoy informatsii // Sovremennyye nauchnyye issledovaniya i innovatsii. 2017. № 8. S. 17.

Авторы заявляют об отсутствии конфликта интересов.
Авторами внесён равный вклад в написание статьи.
The authors declare no conflicts of interests.
The authors have made an equal contribution to the writing of the article.

ССЫЛКА ДЛЯ ЦИТИРОВАНИЯ
Артюхов А.В., Юрин А.М. Оперативно-разыскная характеристика преступлений, совершённых с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации (на примере правоприменительной практики Волгоградской области) // Вестник Калининградского филиала Санкт-Петербургского университета МВД России. 2024. № 2 (76). С. 48-58.