Артюхов Александр Витальевич, заместитель начальника кафедры оперативно-розыскной деятельности и специальной техники Волгоградской академии МВД России, кандидат юридических наук, e-mail: alex.v.artuhov@yandex.ru, ORCID 0000-0001-9344-5241

Юрин Александр Михайлович, начальник ОБК ГУ МВД России по Волгоградской области, полковник полиции.

Оперативно-розыскная характеристика преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации (на примере правоприменительной практики Волгоградской области)

Аннотация.

Введение.

В статье определена необходимость использования как гласных, так и негласных сил средств и методов оперативно-розыскной деятельности. Раскрыты методы противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации в современных условиях. Рассмотрены наиболее значимые элементы оперативно-розыскной характеристики, связанные с данным видом преступных посягательств, в том числе: современное состояние преступности в сфере информационно-телекоммуникационных технологий; обстановка совершения преступления; оперативно-значимые данные о личности киберпреступника и потерпевших; способы совершения преступления и оперативно-розыскная профилактика.

Методы исследования.

В работе применялся общенаучный диалектический метод познания окружающей действительности, предполагающий полное и всестороннее изучение явлений, рассмотрение связей и противоречий между ними. Кроме этого, был использован метод описания; метод логического осмысления.

Проведен анализ статистических данных, характеризующих современное состояние противодействия IT-преступлениям, а также личность киберпреступников.

Результаты.

Наиболее подробно освещены не только существующие способы совершения преступлений рассматриваемой направленности, но и меры оказываемого противодействия сотрудникам оперативных подразделений в современных условиях. Приведена зарубежная практика противодействия рассматриваемым преступлениям. В качестве выводов предложены изменения законодательства, регламентирующего оперативно-розыскную деятельность в данной сфере общественных отношений.

Ключевые слова: информационно-телекоммуникационные технологии, компьютерная информация, оперативно-розыскная деятельность, оперативно-розыскные мероприятия, киберпреступник, компьютерный вирус.

Artyukhov Alexander Vitalievich, Deputy Head of the Department of Operational Investigative Activities and Special Equipment of the Volgograd Academy of the Ministry of Internal Affairs of Russia, Candidate of Law, E-mail: alex.v.artuhov@yandex.ru ORCHID 0000-0001-9344-5241

Yurin Alexander Mikhailovich, Head of the Regional Committee of the Ministry of Internal Affairs of Russia for the Volgograd region, police colonel.

Operational investigative characteristics of crimes committed using information and telecommunication technologies or in the field of computer information (using the example of law enforcement practice in the Volgograd region)

Annotation.

Introduction.

The article defines the need to use both public and secret forces of means and methods of operational investigative activities. The methods of countering crimes committed using information and telecommunication technologies or in the field of computer information in modern conditions are disclosed. The most significant elements of the operational investigative characteristics associated with this type of criminal encroachments are considered, including: the current state of crime in the field of information and telecommunication technologies; the crime scene; operationally significant data on the identity of the cybercriminal and the victims; methods of committing a crime and operational investigative prevention.

Research methods.

The work used a general scientific dialectical method of cognition of the surrounding reality, which involves a complete and comprehensive study of phenomena, consideration of connections and contradictions between them. In addition, the method of description was used; the method of logical comprehension. The analysis of statistical data characterizing the current state of countering IT crimes, as well as the identity of cybercriminals, is carried out.

Results.

The most detailed coverage is given not only to the existing methods of committing crimes of the considered orientation, but also to the measures of counteraction provided to employees of operational units in modern conditions. The foreign practice of countering the crimes in question is given. As conclusions, amendments to the legislation regulating operational investigative activities in this area of public relations are proposed.

Keywords: information and telecommunication technologies, computer information, operational investigative activities, operational investigative measures, cybercriminal, computer virus.

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 - IT-преступления), является одной из центральных в практической ежедневной повестке государства, уполномоченных органов и должностных лиц. Именно вокруг организации противодействия IT-преступлениям во многом формируются программные нормативные документы, призванные бороться с преступностью и обеспечивать безопасность страны. Неслучайно в «Стратегии национальной безопасности Российской Федерации», утвержденной указом Президента РФ от 2 июля 2021 года № 400[1] IT-преступления признаны одной из основных угроз общественной безопасности.

В теории оперативно-розыскной деятельности (далее – ОРД) методика противодействия различным видам преступлений, включая IT-преступления, наиболее полно освещается при раскрытии элементов оперативно-розыскной характеристики. Оперативно-розыскная характеристика преступлений представляет собой одну из наиболее дискуссионных и спорных дефиниций во всей оперативно-розыскной науке. При этом всю совокупность споров относительно данного определения следует разделить на три составляющие, а именно: понятие, содержание и обусловленность существования. Считаем, что прежде, чем начать исследовать вопросы оперативно-розыскной характеристики IT-преступлений, необходимо рассмотреть указанные теоретические вопросы.

[1] О Стратегии национальной безопасности Российской Федерации: указ Президента РФ от 02 июля 2021 № 400 [Электронный ресурс] // СПС Консультант Плюс.

С лингвистической точки зрения под оперативно-розыскной характеристикой преступлений следует понимать совокупность знаний, сведений и информации о преступлении, необходимых субъектам ОРД для качественного и эффективного раскрытия данных противоправных деяний. Безусловно, приведенное определение можно называть абстрактным. Вместе с тем нас интересовала именно семантическая точка зрения, которая в данном случае позволяет определить внешне выраженную сущность исследуемого понятия.

Необходимость существования элементов оперативно-розыскной характеристики преступлений обосновывается фактической невозможностью рассматривать данную дефиницию в общем порядке, без применения структурированного подхода. Очевидно, что содержательно оперативно-розыскная характеристика преступлений представляет собой достаточно объемный массив информации, использование которого без деления ее на составные части невозможно. Подобное не приведет к пониманию сущности исследуемого деяния, и не будет носить прикладного или гносеологического характера.

Обоснованность существования дефиниции «оперативно-розыскная характеристика преступлений» – это, пожалуй, самый существенный дискуссионный вопрос, который можно назвать радикальным, так как он ставит под сомнение само существование оперативно-розыскной характеристики преступлений как самостоятельного явления.

В основу сомнений о необходимости существования исследуемой дефиниции положен следующий аспект. Со своей содержательной стороны оперативно-розыскная характеристика преступлений достаточно сильно схожа с иными видами характеристик преступлений в других юридических науках [1, с. 101]. Особенно это заметно при сопоставлении с криминалистикой характеристикой преступления. Данный факт побуждает некоторых исследователей говорить о том, что оперативно-розыскная

характеристика преступлений выступает новым фантомом ОРД, а, следовательно, ее дальнейшая разработка научной значимости не имеет [2, с. 94]. На наш взгляд, данная 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].

В.Д. Ларичев, признавая схожесть элементов оперативно-розыскной характеристики преступлений с иными видами их характеристик, 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-розыскной характеристики преступлений необходимо определять детерминантную сущность ее использования. Ни одна другая характеристика преступлений не может дать возможность субъекту ОРД спланировать и организовать оперативно-розыскные мероприятия (далее – ОРМ), проводимые как гласно, так и негласно, которые в конечном итоге позволяют раскрыть преступление. Поэтому оперативно-розыскную характеристику преступления, как элемент оперативно-розыскной, поисковой и противоборствующей преступлениям деятельности субъектов ОРД, следует считать важнейшей самостоятельной дефиницией, требующей самого тщательного подхода к своему изучению. В связи с этим, считаем необходимым рассмотреть основные элементы оперативно-розыскной характеристики IT-преступлений.

Учитывая сказанное, можем предположить, что в единую систему (применимую, в том числе и по отношению к преступлениям исследуемой

категории) признаков оперативно-розыскной характеристики преступлений входят следующие элементы:

- современное состояние преступности в сфере ИТТ;

- обстановка совершения преступления;

- оперативно-значимые данные о личности киберпреступника и потерпевших;

- способы совершения преступления;

- оперативно-розыскная профилактика.

О современном состоянии преступности в сфере ИТТ и её актуальности свидетельствует официальная статистика. Так, по данным Главного информационно-аналитического центра МВД России (далее – ГИАЦ МВД России) был зарегистрирован существенный рост таких деяний[2].

Таблица 1.

Количество зарегистрированных IT-преступлений
в России за 2021-2023 годы

Отчетный период	Всего IT-преступлений	Тяжкие и особо тяжкие	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%)

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

− проблема борьбы с IT-преступлениями, остается актуальной;

[2] Состояние преступности в России за 2021-2023 год [Электронный ресурс] // Министерство внутренних дел Российской Федерации: сайт. – URL: https://cdn1.tenchat.ru/static/vbc-gostinder/.pdf (дата обращения: 01.05.2024).

− 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 стала исключением, здесь также наблюдается расширение масштабов совершения IT-преступлений, что влечёт за собой рост причиняемого материального ущерба.

Согласно статистическим данным ИЦ ГУ МВД России по Волгоградской области был зарегистрирован существенный рост таких деяний [3]:

Таблица 2.

Количество зарегистрированных IT-преступлений
в Волгоградской области за 2021-2023 годы

Отчетный период	Всего ИТТ или в сфере компьютерной информации	динамика IT-преступлений или в сфере компьютерной информации	приостановлено категории тяжких и особо тяжких преступлений	ущерб, тыс. руб.
2021	9 769	+1 206	7 797	1 299 134
2022	10 992	+1 223	6 942	925 256
2023	13 636	+2 644	8 532	1 871 600

Вследствие обозначенных угроз, коллегией МВД России[4] в конце 2019 года было принято решение о проведении организационно-штатных мероприятий, направленных на создание в подразделениях по контролю за оборотом наркотиков (далее – ГУКОН МВД России), по противодействию экстремизму (далее – ГУПЭ МВД России), уголовного розыска (далее –

[3] 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.

[4] П. 23 Приказа МВД России от 25 ноября 2019 г. № 878 «Об объявлении решения коллегии Министерства внутренних дел Российской Федерации от 1 ноября 2019 г. № 3км» [Электронный ресурс] // СПС Консультант Плюс.

ГУУР МВД России), экономической безопасности и противодействия коррупции (далее – ГУЭПиПК МВД России), следственных подразделениях (далее – СП МВД России), дознания (далее – УОД МВД России), специальных технических мероприятий (далее – БСТМ МВД России), отделов, отделений, групп, специализирующихся на противодействии IT-преступлениям.

Анализ складывающейся оперативной обстановки свидетельствует, что, несмотря на предпринимаемые государством меры по предотвращению роста IT-преступлений, они оказываются недостаточно эффективными и требуют скорейшего расширения. В этой связи в сентябре 2022 г. в системе МВД России создано Управление по организации борьбы с противоправным использованием информационно-коммуникационных технологий (далее – УБК МВД России)[5]. Рассмотрим специфику организации работы УБК МВД России. В этой связи акцентируем внимание на наиболее значимых, на наш взгляд, направлениях деятельности данного оперативного подразделения, связанных с документированием и раскрытием отдельных видов вышеуказанных преступлений на примере Волгоградской области.

Во-первых, отметим, что указанное оперативное подразделение осуществляет ОРД в полном объеме[6].

Во-вторых, отдел по борьбе с противоправным использованием информационно-телекоммуникационных технологий (далее – ОБК ГУ МВД России по Волгоградской области) был образован 01 февраля 2023 г., а фактически осуществлять ОРД его сотрудники стали с ноября 2023 г.

---

[5]О внесении изменений в некоторые акты Президента Российской Федерации: указ Президента Российской Федерации от 30 сентября 2022 № 688 [Электронный ресурс]; О создании Управления по организации борьбы с противоправным использованием информационно-коммуникационных технологий Министерства внутренних дел Российской Федерации: приказ МВД России от 11 октября 2022 № 747 [Электронный ресурс] // СПС Консультант Плюс.

[6] Об утверждении Перечня оперативных подразделений органов внутренних дел Российской Федерации, правомочных осуществлять оперативно-розыскную деятельность: приказ МВД России от 31.03.2023 № 199 [Электронный ресурс] // СПС Консультант Плюс.

В-третьих, основным задачами ОБК ГУ МВД России по Волгоградской области[7] 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;

- ориентированных на выявление и пресечение деятельности транснациональных, межрегиональных организованных групп и преступных

[7] Об утверждении Положения об отделе по борьбе с противоправным использованием информационно-коммуникационных технологий ГУ МВД России по Волгоградской области: приказ ГУ МВД России по Волгоградской области от 30 марта 2023 г. № 176 [Электронный ресурс] // СПС Консультант Плюс.

сообществ (преступных организаций), совершающих преступления с использованием (в сфере) информационно-коммуникационных технологий;

Таким образом, МВД России был предприняты конкретные меры организационно-правового характера, направленные на определение полномочий оперативных подразделений ОВД России, осуществляющих противодействие IT-преступлениям[8].

Методы исследования.

В работе применялся общенаучный диалектический метод познания окружающей действительности, предполагающий полное и всестороннее изучение явлений, рассмотрение связей и противоречий между ними. Кроме этого, был использован метод описания, необходимый для сбора фактического материала о проблемах, возникающих в процессе противодействия IT-преступлениям; метод логического осмысления, позволивший определить понятие «оперативно-розыскной характеристики преступлений» и его элементы, абстрагирование и обобщение, призванные систематизировать установленные нами факты и дать им толкование. Проведен анализ статистических данных, характеризующих современное состояние противодействия IT-преступлениям, а также личность киберпреступников.

Результаты.

С учетом концепции данной статьи необходимо детально проанализировать соответствующие сведения статистики для оценки эффективности работы подразделений УБК МВД России, осуществляющих

[8] 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 05 апреля 2022 № 236 [Электронный ресурс] // СПС Консультант Плюс; 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»: приказ МВД России от 27 июля 2023 г. № 547 [Электронный ресурс] // СПС Консультант Плюс.

противодействие IT-преступлениям, способы их совершения, а также факторы, влияющие на уровень рассматриваемой преступности. При этом акцентируем внимание на наиболее значимых, на наш взгляд, направлениях деятельности данного оперативного подразделения, связанных с документированием и раскрытием отдельных видов вышеуказанных 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 категория лиц, которая обоснованно считается наиболее уязвимой и незащищенной. 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]. Среди средств совершения преступлений рассматриваемой направленности выступают современные средства коммуникации – социальные сети, электронная почта, мобильные приложения WhatsApp или Viber, интернет-сайты знакомств, форумы и чаты. Одной из основных задач, стоящих перед сотрудниками ОБК ГУ МВД России по Волгоградской области в ходе доказывания вины киберпреступника, является, во-первых, документирование переписки преступника с несовершеннолетним, не достигшим возраста шестнадцати лет. Во-вторых, установление факта использования аккаунта в социальных сетях, посредством которого осуществлялась противоправная деятельность, именно преступником, а не

третьим лицом. При этом данные обстоятельства устанавливаются путем проведения компьютерной экспертизы, а также путем получения информации от владельцев социальных сетей и мессенджеров [6, с. 30].

В качестве положительного примера работы по выявлению и документированию подобных преступлений приведём реализацию материалов ОРД сотрудниками ОБК ГУ МВД России по Волгоградской области в отношении жителя г. Волгограда, ранее не судимого гр. К. Так, в период с августа по октябрь 2023 г. в ходе проведения комплекса ОРМ 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 было возбуждено уголовное дело по признакам преступления, предусмотренного ч. 3 ст. 135 УК РФ, а в отношении гр. К вынесено постановление о привлечении в качестве обвиняемого. Обвиняемый 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, (кроме ст. 159.6 УК РФ), в совокупности со ст. 272 или 273 УК РФ. При анализе данной категории преступлений, входящих в компетенцию ОБК ГУ МВД России по Волгоградской области, следует учесть, что все действия (за исключением статьи 159.6 УК РФ) требуют дополнительной квалификации по статьям 272 и/или 273 УК РФ. Это обусловлено тем, что злоумышленники в процессе совершения IT-преступлений осуществляют неправомерный

доступ к компьютерной информации и (или) создают, используют и распространяют вредоносные компьютерные программы, способные удалять, блокировать или модифицировать компьютерную информацию либо иным образом вмешиваться в работу средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

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

Киберпреступники, играя на неосведомлённости потенциальных жертв (особенно несовершеннолетних и граждан пенсионного возраста) об информационной безопасности, размещающих в большом количестве и свободном доступе данные о себе и родственниках в социальных сетях, мессенджерах и компьютерных играх, отправляют 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. 144-145 УПК РФ. Последствия указанных противоправных деяний создают предпосылки к дестабилизации оперативной обстановки в стране и регионе.

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

Согласно статистике за 2023 г., приведенной ЗАО «Лаборатория Касперского», злоумышленники постоянно создают и используют новые способы распространения вредоносного программного обеспечения и обходят установленные, не отвечающие современным требованиям, способы защиты информации, хранящейся на компьютере. Количество появляющихся новых вредоносных программ доходит до 411 тысяч в день[9]. Кроме того,

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

предметом IT-преступлений является и оборудование, обеспечивающее информационно-телекоммуникационные процессы. Более того, возможности «Интернета» используются представителями спецслужб иностранных государств для организации «цветных революций» и других противоправных действий.

Обобщая сказанное, все IT-преступления условно можно разделить на 2 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 противоправное деяние, которое включает в себя незаконное получение доступа к компьютерной информации без разрешения владельца или пользователя этой информации, образующее состав уголовного преступления.

2. Разработка и распространение компьютерных вирусов.

Компьютерные вирусы были и остаются одной из наиболее распространенных причин потери информации. Известны факты, когда вирусы блокировали работу организаций и предприятий. Так, 25 января 2003 года в США вирусный червь «Slammer» обрушил корпоративную сеть атомной электростанции в штате Огайо, после чего распространился на системы мониторинга безопасности и охлаждения станции. В сентябре 2010 года в Иране около 30тыс. компьютерных систем промышленных объектов были заражены вирусом «Stuxnet». Взлом привел к остановке работы более 1,3тыс. центрифуг по обогащению урана в Натанзеи переносу сроков запуска

АЭС «Бушер»[10]. Также 27 июня 2017 года вирус-вымогатель заблокировал компьютеры радиационного мониторинга Чернобыльской АЭС.[11]

Компьютерный вирус – это программа, которая может копировать себя и распространяться без ведома пользователя, часто нанося вред компьютеру или данным. Вирусы могут быть созданы для различных целей, включая кражу личных сведений, повреждение файлов, нарушение работы компьютера или даже использование компьютера для атаки на другие системы. Основными каналами распространения вирусов являются: электронная почта, интернет-сайты, съемные носители информации и др.

С целью обеспечения информационной безопасности пользователям необходимо использовать различное антивирусное программное обеспечение и быть осторожными при открытии электронных писем или загрузке файлов из ненадежных источников, чтобы предотвратить заражение компьютера вирусом.

3. Ввод в компьютер пользователя вредоносных программ.

Прежде всего – это процесс, при котором 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 способов принято относить следующие: загрузка вредоносного программного обеспечения из «Интернета» при посещении неизвестных сайтов или при загрузке файлов из ненадежных источников; открытие писем в электронной почте, в результате чего пользователь может получить электронное письмо с вложением, которое при его просмотре автоматически устанавливает вредоносное программное обеспечение на его персональный компьютер; установка вредоносного программного обеспечения с помощью съемных носителей информации,

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

[11] Вирус-вымогатель Petya поразил Чернобыльскую АЭС [Электронный ресурс] // РИА-новости: сайт. – URL: https://ria.ru/20170627/1497397238.html (дата обращения: 01.05.2024).

такие как USB-флешки или CD/DVD-диски, на которых установлено вирусное программное обеспечение. установка вредоносного программного обеспечения через уязвимости в операционной системе пользователя или приложениях, например в процессе автоматической установки обновлений операционной системы, браузеров, драйверов на компьютер пользователя. установка вредоносного приложения по средствам техник социальной инженерии, например, когда пользователя вводят в заблуждение либо обманывают или убеждают установить вредоносное программное обеспечение, через фишинговые электронные письма или поддельные сайты.

4. Неправомерное нарушение эксплуатации компьютера, систем компьютеров или их сетей либо в умышленном нарушении установленных правил и процедур.

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

5. Хищение компьютерной информации.

Следует заметить, что доказать классификацию 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 пользователю 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 компьютерной системе, намеренно удаляется или становится недоступной. Это может произойти различными способами, включая действия, в результате которых происходит: удаление файлов с

компьютера, что приводит к их недоступности в результате повреждения; форматирование диска, в результате чего удаляются все данные на нем; уничтожение данных на компьютере, например, путем перезаписи файлов или удаления их из таблицы файлов; уничтожения данных на компьютере или компьютерной системе по средством проведения кибератаки.

7. Подделка компьютерной информации.

Это процесс, при котором информация, хранящаяся на компьютере пользователя либо компьютерной системе, намеренно изменяется или фальсифицируется без ведома или согласия владельца. Данный способ направлен на изменение результатов конечной информации, запрашиваемой заказчиком, например, результат какого-либо конкурса и т.п.

IT-преступления, совершаемые с использованием компьютера.

Анализ второй группы рассматриваемых преступлений позволяет сделать вывод, что компьютеры (переносные (портативные) – ноутбуки, планшетные компьютеры, смартфоны) используется как средство для их совершения. В то же время правоприменительная практика свидетельствует, что данные устройства способны хранить, передавать и обрабатывать информацию, которая необходима для различных противоправных действий [8, с. 145]. В этой связи компьютер необходимо рассматривать как элемент борьбы с IT-преступлениями. В этом контексте он требует особого внимания со стороны оперативных сотрудников ОБК ГУ МВД России по Волгоградской области. Это необходимо для получения доказательной информации и обеспечения надлежащего уголовного судопроизводства.

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

Следующим по значимости элементом оперативно-розыскной характеристики IT-преступлений, является личность киберпреступника. Не случайно исследователи в области криминалистики, криминологии, уголовного права, оперативно-розыскной 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 своих 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 (например, позволяющие создавать простые вредоносные программы или использовать готовые инструменты для совершения IT-преступлений).

Кроме этого, необходимо учитывать тот факт, что киберпреступления могут совершаться единолично либо организованными группами специалистов в области ИТТ, либо 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, во-первых, 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, локализующегося на территории иного государства и, как правило,

недружественного. Кроме того, VPN может скрывать реальный IP-адрес пользователя. Во-вторых, использование киберпреступниками одного из самых надежных способов противодействия правоохранительным органам и легализации доходов от своей преступной деятельности, является перевод денежных средств из официальных платежных систем в различные виды 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». Примененная терминология не случайна. «Дроп» (от англ. drop, сбрасывать) на сленге киберпреступников – это подставное лицо, а карты, на которое они оформлены, соответственно – «дроп-картами».

Анализируя оперативно-значимые данные о личности, нельзя обойти вниманием тот факт, что возраст киберпреступников разный. Некоторые из них – это молодые люди, которые только начинают осваивать компьютерные технологии (например, дети, которые уже с 14-летнего возраста имеют особые навыки и технические возможности для совершения разного рода IT-преступлений) [11, с. 8], другие – это 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 указанных признаков позволяет организовать эффективную работу по предупреждению и раскрытию рассматриваемых преступлений.

Рассматривая последний элемент оперативно-розыскной характеристики, отметим, что помимо мероприятий, направленных на выявление и раскрытие данных преступлений, на подразделения ОБК ГУ

МВД России по Волгоградской области возложены задачи по проведению мер профилактики. В качестве положительных примеров проводимой профилактической работы на территории Волгоградской области можно выделить следующие:

1. Проведение оперативно-профилактического мероприятия (далее – ОПМ) «Сорняк», направленного на выявление, предупреждение, пресечение преступлений и административных правонарушений, связанных с эксплуатацией женщин и детей, а также производством и распространением порнографической продукции, совершаемых с использованием информационных технологий.

2. Доведение до сведения граждан информации, направленной на повышение их цифровой грамотности. Считаем, что это – одна из важнейших задач, которая была обозначена Президентом Российской Федерации В.В. Путиным на заседании коллегии МВД России, состоявшейся в 2023 году. Под словом «грамотность» стоит понимать не только владение навыками пользования операционной системой и назначение функций, но и знание о базовых правилах «гигиены» в интернете, умение обнаруживать угрозы на ранней стадии. Так, минимальные знания о самых распространенных видах атак, может предотвратить возможность совершения преступления.

3. Разработка и распространение методических рекомендаций и алгоритмов действий, содержащих, кроме прочего меры профилактического характера, с целью незамедлительного информирования ОБК ГУ МВД России по Волгоградской области руководителями территориальных органов внутренних дел региона о фактах выявления преступлений против несовершеннолетних, совершенных с использованием ИТТ[12];

4. Участие в рамках созданной рабочей группы на базе Отделения «Волгоград» Южного главного управления ЦБ РФ, в состав которой входят

[12] Методические рекомендации ОБК ГУ МВД России по Волгоградской области от 7 марта 2024 г. № 6/1341 // Архив ОБК ГУ МВД России по Волгоградской области.

сотрудники правоохранительных органов, в том числе прокуратуры, представители кредитно-финансовых организаций, сотовых компаний, и другие заинтересованные субъекты, в части выработки и реализации мер на региональном уровне, направленных на предупреждение рассматриваемых киберпреступлений.

Заключение.

В современных условиях на существующее более года оперативное подразделение УБК МВД России и его структурные подразделения государством возложены задачи по обеспечению безопасности в киберпространстве. На наш взгляд, эффективность данной структуры будет зависеть от реализации нескольких ключевых факторов:

1. Нивелирование несовершенства действующего уголовного законодательства. 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 воспользоваться каким-либо сервисом [13, с. 32].

За изменение идентификационного кода абонентского устройства сотовой связи, создание дубликата сим-карты идентификации абонента сотовой связи, отсутствует уголовная ответственность. Вместе с тем, используя только абонентский 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 указанные действия, предусмотрена. Неслучайно еще в 2013 году были внесены изменения в ФЗ «Об оперативно-розыскной

деятельности» № 144-ФЗ[13] (далее – ФЗ «Об ОРД»), которые наряду с экологической, государственной, экономической безопасностью Российской Федерации поставили информационную безопасность страны и тем самым дали возможность проведения ОРМ всем заинтересованным субъектам, правомочным осуществлять ОРД. Однако, к сожалению, стоит признать, что это не является прямым указанием на возможность проведения ОРМ в сети Интернет. Законодатель в статье 10 ФЗ «Об ОРД» закрепляет лишь возможность создания и использования информационных систем, без какой-либо конкретизации. В этой связи предлагаем дополнить статью 10 ФЗ «Об ОРД» следующим содержанием:

«органы, осуществляющие оперативно-розыскную деятельность, для решения задач, возложенных на них настоящим Федеральным законом, могут создавать и использовать информационные системы, *включая специальное программное обеспечение, обеспечивающего удаленный доступ к устройствам по средствам информационно-телекоммуникационной сети Интернет*, а также заводить дела оперативного учета».

Отметим, что такая практика с успехом апробирована и применяется в странах Европы и США с 2010 года [15, с. 19]. Правоохранительными органами используются программы − помощники «правоохранительные трояны», которые в целях раскрытия и расследования преступлений позволяют получать доступ к устройству лица совершившего, совершающего или готовящего совершение IT-преступлений. В нашей правоохранительной системе такие программы-шпионы не используются, не разрабатываются и не охвачены правовым полем, несмотря на то, что подобное программное обеспечение существует. Так, удаленный доступ к электронным устройствам физических и юридических лиц обеспечивают зарубежные программы

[13] О внесении изменений в Федеральный закон «Об оперативно-розыскной деятельности» и статью 13 Федерального закона «О федеральной службе безопасности: федеральный закон от 21 декабря 2013 г. № 369-ФЗ [Электронный ресурс] // СПС Консультант Плюс.

TeamViewer (бесплатный удаленный контроль с устройств, работающих на базе операционной системы android и windows и др.).

2. Слабое взаимодействие, а в ряде случаев его полное отсутствие 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, организуемых на площадках ООН и других содружествах, в которых состоит Российская Федерация [16, с. 150]. Подчеркнем, что в настоящее время сотрудничество Российских правоохранительных органов в сфере ИТТ в условиях беспрецедентного секционного давления со стороны США и их союзников, связанного с проведением нашей страной специальной военной операции на Украине, возможно только с дружественными странами.

3. Недостаточный потенциал тех, кто занимается 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 проблематику также указали опрошенные респонденты из числа сотрудников оперативных подразделений ГУ МВД России по Волгоградской области, осуществляющих противодействие IT-преступлениям. Считаем необходимым для МВД России заняться подготовкой высококвалифицированных кадров, способных эффективно выявлять, раскрывать и расследовать киберпреступления.

Учет в работе по противодействию IT-преступлениям перечисленных нами факторов поможет решить задачи по обеспечению безопасности в киберпространстве и повысить защищенность наших граждан 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.

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.

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 [Электронный ресурс]: сб. науч. тр. по материалам II Всерос. межвуз. науч.-практ. конф. Волгоград, 06 декабря 2016 г. Вып. 2/ под ред. Н.В. Ходяковой. – Электрон. дан. (3,4 Мб). – Волгоград : ВА МВД России, 2017. – 1 электрон. опт. диск (CD-R). – Систем. требования : IMB PC, 1 GHz ; 512 Мб оперативной памяти

; 3 Мб ОЗУ ; CD/DVDROM дисковод ; операционная система Windows XP и выше ; Adobe Acrobat Reader 8.0 и выше. 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. – EDN SGMALR.

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. – EDN DZACND.

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

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 [Электронный ресурс] : сб. науч. тр. Междунар. науч.-практ. конф., Волгоград, 18-19 мая 2017 г. / редкол. : В. И. Третьяков, В. В. Намнясева, В. А. Канубриков, О. В. Стрилец. – Электрон. дан. (2,8 Мб). – Волгоград : ВА МВД России, 2017. – 1 электрон. опт. диск

(CD-R). – Систем. требования: IBM PC, 1 GHz; 512 Мб оперативной памяти; 3 Мб ОЗУ; CD/DVD-ROM дисковод; операционная система Windows XP и выше; Adobe Acrobat Reader 8.0 и выше. 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. Волгоград: ВА 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. Новые информационные технологии в практике работы правоохранительных органов / К. Т. Ростов, Д. И. Игнатенко, В. В. Бондуровский, Н. Н. Бухаров // Вестник Санкт-Петербургского университета МВД России. – 1999. – № 1(1). – С. 143-153. – EDN NJFMHP.

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

Bibliographic list

1. Katkov S.V., Belokobyl'skaya O.I., Gornyh S.A. Operativno-rozysknaya harakteristika prestuplenij, sovershaemyh v kreditno-finansovoj sfere: otdel'nye voprosy teorii i praktiki // Vestnik Volgogradskoj akademii MVD Rossii. – 2019. – № 2 (49) – S. 100-110.

2. Zaharcev S.I., Kiryushkina N.O. Novye fantomy operativno-rozysknoj deyatel'nosti: operativno-rozysknaya harakteristika i operativno-rozysknoj kodeks // YUridicheskaya nauka: istoriya i sovremennost'. – 2013. – № 9. – S. 94.

3. Lugovik V.F. Problemy formirovaniya ucheniya ob operativno-rozysknoj harakteristike prestuplenij // Operativnik (syshchik). – 2006. – № 4 (9). – S. 13-16.

4. Larichev V.D. Operativno-rozysknaya harakteristika ekonomicheskih prestuplenij: ponyatie i soderzhanie // Operativnik (syshchik). – 2009. – № 1(18). – S. 11-16.

5. Alekseeva A.P., Nichugovskaya O.N. Kiberprestupnost': osnovnye cherty i formy proyavleniya // Prestupnost' v sfere informacionnyh i telekommunikacionnyh tekhnologij: problemy preduprezhdeniya, raskrytiya i rassledovaniya prestuplenij. 2017. №1. S. 27-34.

6. Alekseeva A.P. Kiberprestupnost': naskol'ko real'na ugroza // Nauchno-metodicheskij elektronnyj zhurnal Koncept. 2017. T. 31. S. 76-80.

7. Alekseeva A.P. Perspektivy razvitiya ugolovnogo zakonodatel'stva v kibersfere // Podgotovka sotrudnikov policii k ispol'zovaniyu informacionnyh tekhnologij v bor'be s prestupnost'yu [Elektronnyj resurs]: sb. nauch. tr. po materialam II Vseros. mezhvuz. nauch.-prakt. konf. Volgograd, 06 dekabrya 2016 g. Vyp. 2/ pod red. N.V. Hodyakovoj. – Elektron. dan. (3,4 Mb). – Volgograd : VA MVD Rossii, 2017. – 1 elektron. opt. disk (CD-R). – Sistem. trebovaniya : IMB PC, 1 GHz ; 512 Mb operativnoj pamyati ; 3 Mb OZU ; CD/DVDROM diskovod ; operacionnaya sistema Windows XP i vyshe ; Adobe Acrobat Reader 8.0 i vyshe. S. 24-31.

8. SHahmatov A. V. Bazhukov V. B. Operativno-rozysknoe issledovanie elektronnyh nositelej informacii pri vyyavlenii i raskrytii prestuplenij v kreditno-bankovskoj sfere // Vestnik Sankt-Peterburgskogo universiteta MVD Rossii. – 2014. – № 2(62). – S. 143-147. – EDN SGMALR.

9. Kushnirenko S. P. Harakteristika sub"ekta kak elementa sistemy prestupnogo posyagatel'stva v sfere vysokih tekhnologij // Vestnik Sankt-Peterburgskogo universiteta MVD Rossii. – 2005. – № 4(28-2). – S. 52-60. – EDN DZACND.

10. Karpov, N. O. Predmet nepravomernogo oborota sredstv platezhej (pravovoj i kriminalisticheskij aspekty) / N. O. Karpov // Vestnik Sankt-

Peterburgskogo universiteta MVD Rossii. – 2017. – № 3(75). – S. 119-122. – EDN MWPFLJ.

11. Glazatova S.V., Burceva E.V., Medvedeva S.V. Kiberprestupleniya, sovershaemye nesovershennoletnimi: problemy rassledovaniya // Rossijskij sledovatel'. – 2021. – № 2. – S. 7-10.

12. ZHizhina M.V., Zav'yalova D.V. Lichnost' sub"ekta prestuplenij v sfere komp'yuternoj informacii kak sistemoobrazuyushchij element kriminalisticheskoj harakteristiki (po materialam rossijskih i zarubezhnyh istochnikov) // Aktual'nye problemy rossijskogo prava. – 2022. № 5. – S. 149-158.

13. Alekseeva A.P., Lahin A. N. Zakonodatel'nye iniciativy v sfere uzhestocheniya nakazaniya za hishchenie deneg s bankovskih schetov ili schetov v elektronnyh platezhnyh sistemah // Aktual'nye problemy ugolovnogo zakonodatel'stva na sovremennom etape [Elektronnyj resurs] : sb. nauch. tr. Mezhdunar. nauch.-prakt. konf., Volgograd, 18-19 maya 2017 g. / redkol. : V. I. Tret'yakov, V. V. Namnyaseva, V. A. Kanubrikov, O. V. Strilec. – Elektron. dan. (2,8 Mb). – Volgograd : VA MVD Rossii, 2017. – 1 elektron. opt. disk (CD-R). – Sistem. trebovaniya: IBM PC, 1 GHz; 512 Mb operativnoj pamyati; 3 Mb OZU; CD/DVD-ROM diskovod; operacionnaya sistema Windows XP i vyshe; Adobe Acrobat Reader 8.0 i vyshe. S. 30-34.

14. Katkov S.V., Semenenko G.M., Kostenko N.S., Alekseeva A.P. O merah sovershenstvovaniya organizacii raboty operativnyh i sledstvennyh podrazdelenij MVD Rossii po vyyavleniyu, raskrytiyu i rassledovaniyu hishchenij denezhnyh sredstv s ispol'zovaniem bankovskih kart na territorii Rossijskoj Federacii // Vestnik Volgogradskoj akademii MVD Rossii. Volgograd: VA MVD Rossii, 2020. №4 (55). S. 123-128.

15. Harevich D.L. Neglasnoe rassledovanie v Germanii: Monografiya. − Minsk: Akademiya MVD Respubliki Belarus', 2010. - 287 s.

16. Novye informacionnye tekhnologii v praktike raboty pravoohranitel'nyh organov / K. T. Rostov, D. I. Ignatenko, V. V. Bondurovskij, N. N. Buharov //

Vestnik Sankt-Peterburgskogo universiteta MVD Rossii. – 1999. – № 1(1). – S. 143-153. – EDN NJFMHP.

17. Sin'kov D. A. Povyshenie effektivnosti rassledovaniya prestuplenij v sfere komp'yuternoj informacii // Sovremennye nauchnye issledovaniya i innovacii. – 2017. – № 8. – S. 17.

Представленный материал ранее нигде не публиковался и в настоящее время не находится на рассмотрении на предмет публикации в других изданиях. Заявляем об отсутствии конфликта интересов, связанного с публикацией данной статьи в журнале «Вестник Калининградского филиала Санкт-Петербургского университета МВД России». Разрешаем размещение полнотекстовой версии статьи, а также её частей в открытом доступе в сети Интернет, а также на официальных каналах журнала в социальных сетях. При создании статьи не использовались возможности искусственного интеллекта».

Авторы внесли равный вклад в создание статьи.