На правах рукописи

Зиновьева Нина Сергеевна

КОМПЬЮТЕРНАЯ ИНФОРМАЦИЯ, ПРЕОБРАЗОВАННАЯ МЕТОДАМИ КРИПТОГРАФИИ, В РАСКРЫТИИ И РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ

12.00.12 – криминалистика; судебно-экспертная деятельность;
оперативно-розыскная деятельность

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата юридических наук

Краснодар – 2021

Работа выполнена в федеральном государственном казенном образовательном учреждении высшего образования «Краснодарский университет Министерства внутренних дел Российской Федерации»

Научный руководитель – доктор юридических наук, доцент **Гусев Алексей Васильевич**

Официальные оппоненты: **Грибунов Олег Павлович,** заместитель начальника Восточно-Сибирского института МВД России (по научной работе), доктор юридических наук, профессор;

Лантух Эдуард Владимирович, начальник кафедры криминалистики Санкт-Петербургского университета МВД России, кандидат юридических наук, доцент

Ведущая организация – Московский государственный университет имени М.В. Ломоносова

Защита состоится 28 апреля 2021 г. в 12.30 на заседании диссертационного совета Д 203.017.02 при Краснодарском университете МВД России по адресу: 350005, г. Краснодар, ул. Ярославская, 128, корпус «А4», конференц-зал.

С диссертацией можно ознакомиться в библиотеке Краснодарского университета МВД России.

Полный текст диссертации, автореферат диссертации и отзыв научного руководителя размещены на официальном сайте Краснодарского университета МВД России по адресу: крду.мвд.рф

Автореферат разослан «___» февраля 2021 г.

Ученый секретарь
диссертационного совета  Грибанов Евгений Викторович

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы диссертационного исследования. Создание информационного общества в целом невозможно без формирования культуры обеспечения безопасности в информационном пространстве как у пользователей, так и у владельцев информационных систем и ресурсов. Ключевыми государственными задачами в данном аспекте являются: обеспечение безопасности функционирования информационных и телекоммуникационных систем; развитие технологий защиты информации, обеспечивающих неприкосновенность частной жизни, личной и семейной тайны; безопасность информации ограниченного доступа[1]. В этих целях осуществляется разработка правовых, организационных, технических и экономических мер обеспечения информационной безопасности. Однако реализация комплекса вышеуказанных мер сталкивается с определенными проблемами, поскольку их несовершенство создает условия для использования информационных технологий и телекоммуникационных систем в противоправных целях.

Современные технологии передачи данных позволяют осуществлять удаленное взаимодействие между участниками преступной деятельности, безопасно передавать и хранить сведения о подготовке, совершении и сокрытии преступлений, что предопределяет увеличение числа неочевидных преступлений и позволяет избегать ответственности за совершенные преступные деяния в силу сложностей установления лиц, причастных к их совершению. Сведения, распространяемые посредством информационно-коммуникационных технологий, являются источником криминалистически значимой информации о преступлении, обнаружение, изъятие и исследование которой является необходимым условием для закрепления доказательств в ходе расследования. Несмотря на целенаправленную выработку правоохранительными органами мер противодействия преступным проявлениям в информационно-телекоммуникационной среде, наблюдается рост отдельной категории рассматриваемых преступлений.

Так, в 2019 г. зарегистрировано более 294 тыс. преступлений, совершенных с использованием информационно-телекоммуникацион-

[1] См.: Доктрина информационной безопасности Российской Федерации [Электронный ресурс]: утв. Указом Президента РФ от 5 дек. 2016 г. № 646. URL: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html (дата обращения: 24.04.2020).

ных технологий, что на 70% (!) больше, чем в 2018 г. Половина таких преступлений совершается с использованием сети Интернет, а более трети – посредством мобильной связи. Четыре таких преступления (80,0%) из пяти совершаются путем кражи или мошенничества – 235,5 тыс. (+83,2%), каждое двенадцатое (8,4%) – с целью незаконного производства, сбыта или пересылки наркотических средств – 24,7 тыс. (+31,2%)[2].

Наряду с ростом количественных показателей преступлений в исследуемой сфере, прослеживается тенденция изменения качественных характеристик. Все чаще в целях сокрытия совершаемых преступлений используются методы криптографической защиты данных, передаваемых в информационно-телекоммуникационной сети Интернет, информации, распространяемой посредством сотовой связи, а также информации, хранящейся на электронных носителях. В зависимости от объекта передачи информации применяются определенные методы ее сокрытия, специализированные аппаратно-программные комплексы защиты данных.

Способы и средства криптографической обработки информации разнообразны. Производители программных продуктов и цифровых коммуникационных устройств разрабатывают и интегрируют в них средства криптографической защиты информации личного (конфиденциального) характера, ограничивая таким образом несанкционированный доступ к информации извне. Интернет-сервисы, позволяющие передавать мгновенные текстовые сообщения (а также фото- и видеосообщения), осуществляют шифрование данных между абонентами. Стандартное программное обеспечение, включенное в операционные системы, также позволяет шифровать данные посредством методов криптографии, а компьютерные программы и утилиты, находящиеся в свободном доступе, создают возможность для более эффективного шифрования хранящейся информации.

С учетом этого при раскрытии и расследовании преступлений возникает особая задача выявления компьютерной информации, преобразованной методами криптографии, и ее анализа с целью получения криминалистически значимых данных.

---

[2] См.: Официальные статистические данные Министерства внутренних дел Российской Федерации за 2019 год [Электронный ресурс]. URL: https://мвд.рф/reports/item/19412450 (дата обращения: 24.04.2020).

В настоящее время на государственном уровне проводится активная разработка механизмов правового регулирования отношений в сфере обращения данных, защищаемых методами криптографии. Прежде всего, эти меры направлены на закрепление необходимости хранения операторами связи и провайдерами передаваемых абонентами сообщений и предоставления ключей шифрования по запросам правоохранительных органов. Однако до настоящего времени остается много нерешенных вопросов, связанных с порядком реализации соответствующих предписаний, что объективно снижает эффективность организации взаимодействия с указанными субъектами при раскрытии и расследовании преступлений.

Специфика работы с информацией, сокрытой методами криптографии, свидетельствует о необходимости выработки действенных мер по преодолению законными средствами и методами систем ее защиты, разработки вопросов эффективного взаимодействия субъектов раскрытия и расследования преступлений с соответствующими специалистами, а также компаниями – разработчиками программных продуктов, операторами связи, интернет-провайдерами. Правоприменительная практика уже имеет положительные примеры такой совместной работы, которая, тем не менее, не системна и носит по большей степени локальный характер, что не обеспечивает эффективное решение задач предварительного расследования.

К числу основных проблем, связанных с получением и анализом компьютерной информации рассматриваемого вида, относится отсутствие криминалистических рекомендаций по раскрытию и расследованию преступлений, механизм совершения которых предполагает использование методов шифрования. Это обусловливает необходимость разработки научно обоснованных рекомендаций, которые будут содержать сведения об алгоритмах работы субъектов предварительного расследования по обнаружению, изъятию и использованию такой информации в процессе собирания доказательств.

В научной криминалистической литературе подробно исследованы вопросы получения и использования информации с электронных носителей как в рамках проведения оперативно-розыскных мероприятий, так и в рамках производства отдельных следственных действий; изучены правовые и организационно-тактические аспекты взаимодействия субъектов расследования со специалистами при работе с данными. Однако проблемы, связанные с получением и анализом криминали-

стически значимой компьютерной информации, защищенной методами криптографии, в комплексе не исследовались. Субъекты раскрытия и расследования преступлений не располагают теоретическими разработками и тактико-криминалистическими рекомендациями об особенностях отражения информации о данных, подвергшихся криптографической защите, средствах и методах, используемых для получения такой информации, особенностях взаимодействия субъектов криминалистической деятельности при получении и анализе криптографически защищенной компьютерной информации.

Таким образом, актуальность темы определяется:

существенным расширением объемов криминалистически значимой компьютерной информации, преобразованной методами криптографии, постоянным совершенствованием этих методов и повышением доступности предлагаемых для их реализации средств;

необходимостью выявления и криминалистического анализа криптографически защищенной компьютерной информации в раскрытии, расследовании и предупреждении преступлений, совершаемых с использованием информационно-телекоммуникационных технологий;

несовершенством правового регулирования отношений, возникающих при необходимости доступа к информации, преобразованной методами криптографии, при раскрытии и расследовании преступлений;

неготовностью сотрудников оперативных подразделений и следователей к практическому решению соответствующих задач;

отсутствием теоретических и методических разработок, направленных на повышение эффективности выявления и анализа информации, преобразованной методами криптографии, при раскрытии и расследовании преступлений, в том числе за счет внедрения криптоаналитических аппаратно-программных комплексов, применение которых способно повысить раскрываемость преступлений отдельных видов.

Степень разработанности темы диссертационного исследования. В основу исследования проблем получения и анализа информации, преобразованной методами криптографии, были положены результаты научных изысканий, отражающих сущность информации, принципы ее отражения, тактико-криминалистические приемы анализа и использования полученных данных в ходе раскрытия и расследования преступлений.

Указанные аспекты исследованы в работах Р.С. Белкина, Т.В. Аверьяновой, Е.Р. Россинской, В.А. Жбанкова, В.Г. Булгакова, Е.П. Ищенко, А.Ф. Волынского, А.И. Винберга, С.П. Митричева, В.А. Образцова, И.М. Комарова, О.С. Кучина, А.Ю. Головина, А.В. Варданяна, С.И. Коновалова, Ф.Г. Аминева, Ю.П. Гармаева и др.

Изучением отдельных аспектов получения и анализа информации, распространяемой в информационно-телекоммуникационной среде, занимались такие ученые, как В.Б. Вехов, А.Л. Осипенко, В.А. Мещеряков, А.Н. Яковлев, Н.Н. Федотов и др.

Компьютерная информация являлась предметом исследований диссертаций на соискание ученой степени кандидата наук А.Н. Колычевой (Москва, 2019), А.С. Вражновой (Москва, 2015), К.А. Нелюбина (Екатеринбург, 2016), А.Б. Максимович (Москва, 2018), И.Е. Мазурова (Ростов-на-Дону, 2017), Е.Г. Кравец (Волгоград, 2016), В.Н. Цимбала (Краснодар, 2019), Е.С. Шевченко (Москва, 2016), В.В. Коломинова (Иркутск, 2017), О.А. Решетняк (Волгоград, 2019) и др.

Вместе с тем до настоящего времени не проводилось комплексного исследования, посвященного проблемам получения и анализа криминалистически значимой компьютерной информации, передаваемой посредством информационно-телекоммуникационных систем либо хранящейся на электронных носителях, преобразованной методами криптографической защиты, а также ее использования при расследовании преступлений.

Объектом исследования являются противоправная деятельность лиц, осуществляющих сокрытие криминалистически значимой компьютерной информации путем применения методов ее криптографической защиты, а также общественные отношения, возникающие в процессе выявления, анализа и использования в ходе предварительного расследования такой информации.

Предметом исследования являются закономерности формирования и отражения компьютерной информации, преобразованной методами криптографии, при совершении преступлений, а также особенности ее выявления, получения, анализа и использования в ходе раскрытия и расследования преступлений.

Цель и задачи исследования. Цель диссертационного исследования заключается в разработке комплексной методики обнаружения, фиксации, изъятия и использования субъектами раскрытия и рассле-

дования преступлений компьютерной информации, преобразованной методами криптографии.

Цель исследования предопределила необходимость решения следующих **задач**:

на основе исследования природы возникновения информации, ее места в системе криминалистических знаний, сущности информации, преобразованной методами криптографии, ее значения для раскрытия и расследования преступлений сформулировать определение компьютерной информации, преобразованной методами криптографической защиты;

разработать типологию объектов хранения, учета и обработки компьютерной информации, преобразованной методами криптографии;

сформулировать предложения по совершенствованию правовых норм, которые позволят повысить эффективность реализации тактико-криминалистических приемов обнаружения и изъятия компьютерной информации, преобразованной методами криптографии;

сформулировать криминалистическую характеристику средств сокрытия компьютерной информации, используемых для криптографической защиты данных в преступных целях;

разработать типологию компьютерной информации, преобразованной методами криптографии, имеющей криминалистическое значение, выявить закономерности механизма следообразования с целью определения типичных мест концентрации указанной компьютерной информации;

сформулировать рекомендации по организации взаимодействия субъектов раскрытия и расследования преступлений со специалистами негосударственных экспертных учреждений и компаниями – разработчиками специализированных аппаратно-программных комплексов при выявлении и изъятии компьютерной информации, преобразованной методами криптографии;

разработать тактико-криминалистические рекомендации по проведению отдельных следственных действий с целью обнаружения, изъятия и фиксации компьютерной информации, преобразованной методами криптографии;

разработать рекомендации по использованию аппаратно-программных комплексов и специализированных компьютерных программ субъектами расследования с целью получения компьютерной информации, преобразованной методами криптографии.

Методология и методика исследования. Методологической основой исследования является диалектический метод как общенаучный метод познания объективной действительности. При проведении диссертационного исследования применялись общенаучные и частнонаучные методы теоретического и эмпирического познания, в том числе наблюдение (при изучении природы возникновения и распространения информации в телекоммуникационных сетях и выявлении особенностей ее отражения в информационной среде), описание (закономерностей механизма следообразования при специфичности отражения информации); методы социологического исследования применялись при анкетировании 163 сотрудников оперативных и следственных подразделений органов внутренних дел. Для выявления основных проблем и способов их практического разрешения использовались методы анализа и синтеза в ходе изучения точек зрения ученых-криминалистов, специалистов в сфере уголовно-процессуального права по основным аспектам исследуемой темы, в процессе изучения и обобщения материалов судебной практики. Кроме того, в процессе изучения заявленной темы использовались сравнительно-правовой метод и метод системного исследования.

Нормативной базой исследования выступают Конституция Российской Федерации, федеральные законы, определяющие порядок обращения криптографически преобразованной информации, а также обращения криптографических средств и методов в деятельности государственных органов, организаций и частных лиц, административное и уголовное законодательство, Уголовно-процессуальный кодекс Российской Федерации, федеральные законы «Об оперативно-розыскной деятельности», «О государственной судебно-экспертной деятельности в Российской Федерации», постановления Пленума Верховного Суда Российской Федерации по вопросам правоприменения при обращении информации, ведомственные и межведомственные инструкции и приказы.

Теоретической основой исследования послужили научные труды ученых-криминалистов, а также ученых в области уголовного процесса и оперативно-розыскной деятельности, в которых отражены различные аспекты выявления, получения, оценки и использования криминалистически значимой информации в ходе раскрытия, расследования и предотвращения преступлений, в том числе совершаемых в сфере информационно-телекоммуникационных технологий. Кроме того, были изучены

отдельные результаты исследований в области криптологии, информатики и других, смежных с ними отраслей научного знания.

Эмпирическая база исследования. Достоверность и обоснованность положений, выводов и рекомендаций, содержащихся в диссертационном исследовании, обеспечиваются эмпирическими данными. Так, в основу эмпирического обобщения положены результаты анкетирования 163 сотрудников оперативных подразделений, следственных подразделений органов внутренних дел, которые специализировались на расследовании преступлений, совершаемых как в сфере информационно-телекоммуникационных технологий, так и с их использованием.

В рамках изучения судебно-следственной практики проанализированы 64 вступивших в силу приговора судов, содержащих основные сведения по проблеме проводимого исследования.

Кроме того, в диссертации использовались результаты эмпирических исследований по смежным проблемам, нашедшим отражение в диссертационных работах и научных публикациях ученых-криминалистов, ученых в области уголовного права, уголовного процесса и оперативно-розыскной деятельности.

Новизна научного исследования заключается в том, что в нем сформирована научно обоснованная методика обнаружения, фиксации, изъятия и анализа компьютерной информации, преобразованной методами криптографии, субъектами раскрытия и расследования преступлений в ходе предварительного следствия. Автором сформулированы и уточнены отдельные понятия, имеющие существенное значение для науки криминалистики, в частности «компьютерная информация, преобразованная методами криптографии», «электронный след». Выявлены свойства и признаки компьютерной информации, преобразованной методами криптографии, определены особенности ее отражения. Сформулированы предложения по совершенствованию механизма обнаружения, фиксации, изъятия и исследования обозначенной информации в ходе предварительного расследования.

Выявлены важные организационные особенности взаимодействия субъектов предварительного расследования с учетом складывающихся следственных ситуаций, в рамках которых осуществляются обнаружение и анализ криптографической информации.

Автором разработаны рекомендации по тактике проведения отдельных следственных действий с учетом специфики сокрытия ком-

пьютерной информации криптографическими методами, определены значимые особенности технико-криминалистического обеспечения получения компьютерной информации, преобразованной методами криптографии.

Основные положения, выносимые на защиту. В диссертационном исследовании, которое носит теоретико-прикладной характер, сформулированы и выносятся на защиту следующие положения, выводы и рекомендации, являющиеся новыми или имеющие элементы научной новизны:

1. В условиях цифровизации практически всех сфер жизнедеятельности общества существенно расширяется использование в преступной деятельности компьютерной информации, преобразованной методами криптографии, которая содержит значительный объем криминалистически значимых сведений, способствующих повышению эффективности раскрытия и расследования преступлений. С учетом этого система криминалистических знаний должна быть дополнена новыми уточненными данными о сущности и значении такой информации, особенностях ее отражения и познания с целью использования в ходе раскрытия и расследования преступлений.

Для формирования соответствующей теоретической основы предложено авторское определение компьютерной информации, преобразованной методами криптографической защиты, под которой предлагается понимать передаваемые по телекоммуникационным сетям или зафиксированные на электронном носителе данные, исходная информация которых подвержена шифрованию, стеганографии или кодированию посредством специализированных аппаратно-программных комплексов, функционирующих на основе криптографических алгоритмов, с целью обеспечения ее конфиденциальности.

2. Объектами хранения, учета и обработки компьютерной информации, преобразованной методами криптографии, являются аппаратно-программные средства, функционирующие во взаимодействии четырех основных элементов: а) накопителей информации; б) рабочих станций; в) инфраструктуры, обеспечивающей связь между ними; г) системы управления.

К объектам, подлежащим криптографическим преобразованиям, относятся:

I. Файлы, созданные в средствах автоматизированной обработки информации:

файлы – источники информации, образующиеся в ходе деятельности пользователей (текстовые документы с любым видом форматирования, электронные таблицы, файлы изображений, файлы видеозаписей, файлы аудиозаписей, файлы, хранящие электронные сообщения, файлы, формирующие строение интернет-страницы);

файлы, обеспечивающие аутентификацию и конфиденциальность пользователей (электронный сертификат, электронная ключевая информация, сетевые протоколы).

II. Файлы в средствах сотовой связи, образующиеся в ходе коммуникативной активности пользователей (текстовые документы с любым видом форматирования, файлы изображений, файлы видеозаписей, файлы аудиозаписей, файлы, хранящие электронные сообщения, файлы, формирующие строение интернет-страницы, файлы в приложениях, установленных на устройство сотовой связи).

3. Сокрытие компьютерной информации методами криптографии осуществляется путем применения специализированных аппаратно-программных комплексов.

Под средствами сокрытия компьютерной информации в целях совершения преступления следует понимать компьютерную технику (персональный компьютер, ноутбук, планшетный компьютер) и устройства мобильной связи, функционирующие на основе операционных систем, с установленными на них программными комплексами, позволяющими зашифровывать данные, имеющие значение для выявления, раскрытия, расследования и предупреждения преступлений.

4. При выявлении и анализе компьютерной информации, преобразованной методами криптографии, особое криминалистическое значение приобретают цель преобразования (шифрования) данных и их характеристика.

Основными целями применения методов криптографического преобразования данных являются: а) ограничение доступа к данным, хранящимся непосредственно в компьютере или на внешнем накопителе; б) сокрытие сведений об IP-адресе и MAC-адресе абонента при выходе в сеть Интернет и передаче сведений, содержащих признаки преступления; в) получение дохода от осуществления противоправной деятельности путем перевода на виртуальный счет криптовалюты.

Анализ механизма следообразования позволяет установить типичные места концентрации данных, подверженных криптографической защите, к которым отнесены: а) текстовые, голосовые, фото- и

видеосообщения, передаваемые через сервис мгновенного обмена данными; б) данные, передаваемые посредством электронных почтовых сервисов; в) данные, хранящиеся на компьютерах (на локальных или удаленных серверах) в виде пользовательских или системных файлов; г) данные, распространяемые посредством блокчейн-технологии. В них концентрируется криминалистически значимая информация (сообщения, координирующие преступную деятельность; изображения с детской порнографией; теневая бухгалтерская отчетность и т. п.).

5. Своевременность обнаружения и изъятия компьютерной информации, преобразованной методами криптографии, непосредственно зависит от правильно организованного взаимодействия субъектов раскрытия и расследования преступлений на ведомственном и межведомственном уровнях. Особую роль в ходе раскрытия и расследования преступлений рассматриваемого вида играет взаимодействие с сотрудниками компаний – разработчиков аппаратно-программных средств криптографической защиты компьютерной информации или профильными специалистами негосударственных экспертных учреждений с целью установления криминалистически значимых сведений. В этом случае возникает третий уровень взаимодействия – вневедомственный.

6. Специфика отражения и мест концентрации компьютерной информации, преобразованной методами криптографии, предопределяет необходимость соблюдения ряда криминалистических рекомендаций по ее обнаружению, фиксации и изъятию путем проведения таких следственных действий, как осмотр места происшествия, осмотр предметов и документов, обыск и выемка. Соответствующие криминалистические рекомендации носят как общий характер для всех следственных действий, так и частный для отдельных следственных действий.

Общими тактическими рекомендациями являются следующие: а) любые действия с компьютерной информацией нужно осуществлять под контролем субъекта расследования; б) при изъятии и исследовании информации применяется лицензионное специализированное программное обеспечение; в) обнаружение и изъятие указанной информации должно осуществляться лицами, имеющими знания основ работы с данными; г) перед началом работы по отысканию и изъятию информации необходимо устранить возможность удаленно-

го уничтожения или преобразования компьютерной информации посредством компьютерных сетей; д) любые действия по обнаружению, изъятию и исследованию информации подлежат обязательной видеофиксации.

Наряду с отысканием информации, хранящейся на электронных носителях (компьютерные жесткие диски, смартфоны, внешние средства накопления данных), следует обеспечить обнаружение и исследование средств негласного наблюдения, черновых записей, содержащих сведения о методах и средствах, примененных для криптографической защиты данных, и пароли для доступа к данным.

7. Для обнаружения объектов – носителей криминалистически значимой компьютерной информации, а также для фактического выявления зашифрованных данных, которые содержат вышеуказанные объекты, производится следственный осмотр. Его объектами являются: средства компьютерной техники и элементы сетевой структуры; служебные журналы программ, используемых в рассматриваемых целях; средства хранения информации.

Рабочий этап следственного действия выражается в осуществлении общего и детального осмотра указанных объектов. В рамках общего осмотра осуществляются: а) осмотр и описание в протоколе следственного действия общего состояния устройств (их характеристики и состояние на момент осмотра; включены или выключены); б) изучение способов подключения устройств (проводные или беспроводные) к сетям (их характеристики), наличие периферийных устройств и их функциональное назначение, также устанавливается провайдер, предоставляющий услуги связи и доступа к Интернету.

Детальный осмотр предполагает: а) осмотр аппаратного содержимого внутренних и внешних жестких дисков, а также сетевых карт, которые содержат сведения о программном обеспечении, применяемом для сокрытия или преобразования (видоизменения) данных; б) определение программного обеспечения, используемого для работы с электронными кошельками или криптовалютами; в) изучение программ, содержащих сведения об IP- или MAC-адресах устройств; г) осмотр и исследование браузеров, установленных на устройства; д) осмотр содержимого электронной почты пользователя на предмет выявления криминалистически значимых сведений; е) осмотр и исследование средств синхронизации данных или облачного хранилища, к числу которых могут быть отнесены Dropbox, OneDrive, Яндекс.Диск и др.

8. Основная цель технико-криминалистического обеспечения получения компьютерной информации, преобразованной методами криптографии, выражается в непосредственном использовании субъектами расследования мобильных аппаратно-программных комплексов и специализированных компьютерных программ, позволяющих обходить блокировки в виде паролей и пин-кодов, восстанавливать удаленные данные, расшифровывать криптографические контейнеры, а также извлекать данные из облачных сервисов при отсутствии сведений об учетных данных пользователя. Результатом применения технико-криминалистических средств является возможность дальнейшего преобразования компьютерной информации в доступную для восприятия форму, ее изъятия и анализа.

Теоретическая и практическая значимость диссертационного исследования. Теоретическая значимость работы заключается в разработке научных основ отражения криминалистически значимой компьютерной информации, преобразованной методами криптографической защиты. Результаты научного исследования могут стать основой для дальнейшего изучения проблем использования криминалистических средств и методов получения, исследования и оценки компьютерной информации, преобразованной методами криптографической защиты, в раскрытии и расследовании преступлений.

Изложенные в диссертационном исследовании положения и выводы вносят значительный вклад в развитие теории криминалистики, судебной экспертизы и оперативно-розыскной деятельности. Практическая значимость проведенного исследования заключается в возможности использования его результатов при разработке учебно-методических материалов по дисциплине «Криминалистика», а также специальных криминалистических курсов.

Материалы и выводы диссертационного исследования могут быть применены в качестве методических рекомендаций при осуществлении деятельности по получению и анализу криминалистически значимой компьютерной информации, преобразованной методами криптографии, в целях раскрытия и расследования преступлений, в рамках повышения квалификации и переподготовки кадров, в нормотворческом процессе.

Степень достоверности результатов исследования. Теоретическая часть научного труда базируется на использовании широкого круга российских и зарубежных правовых источников, научной и

учебной литературы, опубликованных материалов конференций различных уровней, а также диссертационных исследований других авторов. Научные выводы и положения основываются на анализе теоретической части исследования, результатах обобщения и анализа эмпирической базы. При разработке научных положений использованы современные методики сбора, обработки и анализа эмпирического материала. Степень достоверности результатов проведенного исследования обеспечена также результатами апробирования разработанных выводов и положений на практике и в учебном процессе, что подтверждается актами внедрения.

Апробация и внедрение результатов исследования. Результаты диссертационного исследования внедрены в деятельность практических органов внутренних дел: Главного следственного управления при Главном управлении МВД России по Иркутской области, Центра по противодействию экстремизму Главного управления МВД России по Краснодарскому краю. Результаты исследования также внедрены в деятельность образовательных организаций МВД России: Краснодарского университета МВД России, Восточно-Сибирского института МВД России, Ростовского юридического института МВД России.

Основные положения диссертационного исследования изложены в 23 научных статьях, из которых 5 опубликованы в изданиях, рекомендованных Высшей аттестационной комиссией при Министерстве науки и высшего образования Российской Федерации для опубликования основных научных результатов диссертаций, и в 2 пособиях. Общий объем опубликованных работ составил 14,5 п. л.

Основные теоретические положения докладывались на научно-представительских мероприятиях различных уровней: Международной научно-практической конференции «Юридическая наука и практика (трибуна молодых ученых)» (Нижний Новгород, 2014); II Всероссийской научной конференции «Актуальные вопросы науки и практики» (Краснодар, 2014); Международной научно-практической конференции «Преступность в СНГ: проблемы предупреждения и раскрытия преступлений» (Воронеж, 2015); XIX Международной выставке средств обеспечения безопасности государства «Интерполитех-2015» (Москва, 2015); Всероссийской научно-практической конференции «Актуальные проблемы уголовного процесса и криминалистики» (Краснодар, 2015); Всероссийской научно-практической конференции «Актуальные проблемы правоохранительной деятельности глазами

молодых ученых» (Симферополь, 2016); Всероссийской научно-практической конференции «Актуальные проблемы борьбы с преступностью» (Волгоград, 2016); V Всероссийской научно-практической конференции «Криминалистика и судебно-экспертная деятельность в условиях современности» (Краснодар, 2017); XXIII Международной научно-практической конференции «Деятельность правоохранительных органов в современных условиях» (Иркутск, 2018); Всероссийской научно-практической конференции «Белгородские криминалистические чтения» (Белгород, 2018); Всероссийской научно-практической конференции «Современные проблемы криминалистики и оперативно-розыскной деятельности» (Ростов-на-Дону, 2019); VII Международной научно-практической конференции «Криминалистика: теория и практика» (Краснодар, 2019); Всероссийской научно-практической конференции «Актуальные проблемы уголовного процесса и криминалистики» (Краснодар, 2020).

Структура диссертации соответствует теме и логике проведенного исследования. Работа содержит введение, две главы, включающие семь параграфов, заключение, список литературы, приложения.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** обосновывается актуальность темы исследования, определяются его объект, предмет, цели и задачи, характеризуются методологические и методические основы работы, ее теоретическая и эмпирическая базы, формулируются основные положения, выносимые на защиту, раскрывается научная новизна диссертации, ее теоретическое и практическое значение, приводятся сведения об апробации и внедрении научных результатов.

Первая глава **«Теоретические основы компьютерной информации, преобразованной методами криптографии, в криминалистике»** содержит три параграфа.

В первом параграфе ***«Развитие научных представлений об информации и их место в криминалистике»*** исследуется генезис теории информации. Подчеркивается, что востребованность информационных отношений распространилась на все сферы деятельности социума. Исключением не стал и криминальный аспект их реализации, в связи с чем потребовались новые эффективные криминалистические подходы к разработке рекомендаций по раскрытию, расследо-

ванию и предупреждению преступлений, совершаемых при помощи информационно-телекоммуникационных технологий.

Во многих случаях реализация информационных отношений в преступной среде осуществляется с использованием специализированных криптографических методов, позволяющих зашифровывать информацию с целью сокрытия ее криминалистически значимого содержания, однако выявление такой информации правоохранительными органами в настоящее время затруднено. Одной из главных причин этого является отсутствие в криминалистической науке эффективных рекомендаций по выявлению криптографической информации, ее исследованию и использованию в правоохранительных целях. Учитывая данную проблему, автор изучил процессы обмена информацией (ее хранения) в преобразованном методами криптографии виде.

В параграфе сформулировано авторское определение компьютерной информации, преобразованной криптографическими методами, под которой следует понимать передаваемые по телекоммуникационным сетям или зафиксированные на электронном носителе данные, в которых исходная информация подвержена шифрованию, стеганографии или кодированию посредством специализированных аппаратно-программных комплексов, функционирующих на основе криптографических алгоритмов, с целью обеспечения ее конфиденциальности.

Во втором параграфе ***«Основы криптографической защиты компьютерной информации в системе криминалистических знаний»*** обосновывается необходимость изучения основ криптографии субъектами раскрытия и расследования преступлений. Автором проведено исследование основных четырех групп методов криптографического преобразования информации (по виду воздействия на исходную информацию): кодирования, шифрования, сжатия, стеганографии. Установлено, что преобразованная или скрытая обозначенными методами информация формирует специфическую следовую картину с определенным набором знаков.

Поскольку в криминалистической науке нет единого понятия следа, отражаемого в электронном информационном пространстве, нет единого мнения в вопросе природы данных следов, а также их места в криминалистической классификации следов преступления, в работе высказано предложение по уточнению понимания сущности электронно-цифрового следа. Кроме того, высказаны рекомендации

по обнаружению и изъятию информационных данных, имеющих криминалистическое значение, преобразованных методом криптографии.

В основу этих рекомендаций положены способы криптографических преобразований информации, осуществляемых в преступных целях, к которым следует отнести: кодирование, шифрование, сжатие и стеганографию. Каждый из приведенных способов преобразования предопределяет закономерный механизм следообразования, познание которого происходит через применение методов криминалистической диагностики.

Компьютерная информация, преобразованная методами криптографии, приобретает криминалистическое значение следа только при условии ее материально фиксированного отражения на цифровом носителе, когда ее модификация, копирование или блокировка возможны посредством криптографического ключа.

В третьем параграфе ***«Компьютерная информация, преобразованная методами криптографии, как средство совершения и сокрытия преступлений»*** для выявления криминалистически значимых свойств и признаков компьютерной информации, преобразованной методами криптографии, определены виды технических средств, в которых используются защищенные данные: 1) компьютерная техника (персональный компьютер, ноутбук, планшет); 2) средства мобильной связи, функционирующие на основе операционных систем, с установленными на них программными комплексами. Основной характеристикой этих средств является возможность преобразовывать, видоизменять и зашифровывать данные, имеющие значение для выявления, раскрытия, расследования и предупреждения преступлений.

Соискателем рассмотрены цели использования правонарушителями типичных методов сокрытия информации:

ограничение физического доступа к данным, хранящимся непосредственно в компьютере или внешнем накопителе;

сокрытие сведений об IP-адресе абонента при выходе в сеть Интернет и передаче сведений, содержащих признаки преступления;

получение прибыли за осуществление противоправной деятельности путем перевода на виртуальный счет криптовалюты.

В работе отмечено, что следы противоправной деятельности проявляются в данных, отраженных в виде текстовых, голосовых, фото- и видеосообщений и передаваемых посредством сервисов мгновен-

ных сообщений, в сервисах электронной почты, облачных хранилищах, а также в данных, хранящихся в компьютерах в виде файлов, документов, фото- и видеоизображений. Отдельно следует отметить данные (чаще всего связанные с обращением криптовалют), распространяемые посредством блокчейн-технологии.

Вторая глава **«Прикладные аспекты использования компьютерной информации, преобразованной методами криптографии, в ходе собирания доказательств»** содержит четыре параграфа.

В первом параграфе ***«Особенности правоотношений, возникающих в сфере обращения компьютерной информации, преобразованной методами криптографии»*** рассматривается деятельность государства, которая направлена на защиту конституционных прав и свобод граждан в информационном поле (сохранение права на тайну переписки) путем разработки эффективных механизмов их обеспечения, при этом принимается во внимание международный опыт. Одним из средств сохранения персональных данных и конфиденциальных сведений является криптографическая защита; разработка таких средств осуществляется в соответствии с правовыми нормами и под надзором органов государственной власти. Однако ограничение конституционных прав граждан со стороны правоохранительных органов продиктовано необходимостью пресечения преступных действий, раскрытия и расследования преступлений, криминалистически значимые сведения о которых содержатся в сообщениях, фото- и видеоизображениях, файлах и т. д., имеющих разные уровни криптографической защиты.

Автором отмечено, что разрабатываемые правовые механизмы в большей степени регулируют деятельность провайдеров и операторов сетей в сфере накопления и предоставления данных. В частности, в настоящее время определены условия их взаимодействия с органами государственной власти, степень ответственности за неисполнение правовых предписаний. Однако по-прежнему открытыми остаются проблемы пресечения деятельности граждан, использующих анонимайзеры, VPN, TOR, программы криптографической защиты данных в целях совершения и сокрытия преступлений, отсутствия меры уголовно-правовой ответственности за вышеуказанные действия, а также несовершенства уголовно-процессуального законодательства в части получения компьютерной информации, преобразованной методами криптографии.

Поскольку наличие этих проблем оказывает непосредственное влияние на доступ правоохранительных органов к имеющей криминалистическое значение информации, скрытой при помощи методов криптографии, автором предложены дополнения и изменения в нормы уголовного и уголовно-процессуального законодательства.

Во втором параграфе ***«Организационные и правовые вопросы взаимодействия субъектов раскрытия и расследования преступлений с целью получения компьютерной информации, преобразованной методами криптографии»*** отмечено, что выявление и получение криминалистически значимой компьютерной информации, преобразованной криптографическими методами, осуществляется эффективно в условиях согласованной по целям и задачам деятельности субъектов раскрытия и расследования преступлений, а также организаций, предоставляющих услуги связи и Интернета, специалистов из числа сотрудников компаний – разработчиков аппаратно-программных криптографических комплексов.

Организационные и правовые аспекты рассматриваемого взаимодействия имеют определенную специфику, обусловленную характерным кругом решаемых частных задач субъектов такой деятельности. В первую очередь, данное взаимодействие определяется требованием собирания, исследования и использования компьютерной информации, преобразованной методами криптографии. Эта информация, являясь по своей сути зашифрованной, требует специализированного подхода взаимодействующих субъектов не только к ее получению, но и к дальнейшему исследованию при помощи специальных знаний.

С учетом сложностей работы по получению криптографической компьютерной информации в работе определяются имеющиеся проблемы правового регулирования рассматриваемого взаимодействия и организации работы взаимодействующих сторон предварительного расследования. В зависимости от круга решаемых задач, процессуального положения субъектов взаимодействия и стадий процессуальной и оперативно-розыскной деятельности выделены ведомственный, межведомственный и вневедомственный уровни взаимодействия, определяемые условиями правового регулирования данной деятельности и особенностями ее организации в процессе раскрытия и расследования преступлений с целью получения компьютерной информации, преобразованной методами криптографии.

В третьем параграфе ***«Особенности тактики проведения отдельных следственных действий с целью отыскания, фиксации и исследования информации, преобразованной методами криптографии»*** автор подчеркивает, что, несмотря на то, что исследованию вопросов производства следственных действий при раскрытии и расследовании преступлений в сфере информационно-телекоммуникационных технологий посвящено достаточное количество работ, системных научно обоснованных рекомендаций по получению компьютерной информации, преобразованной методами криптографии, не разработано. Поэтому в работе предпринята попытка сформулировать эффективные тактико-криминалистические рекомендации по проведению следственных действий с целью отыскания, фиксации и исследования компьютерной информации, преобразованной методами криптографии.

При разработке рекомендаций учитывались специфические особенности отыскания, фиксации и исследования компьютерной информации, преобразованной методами криптографии. Так, в первую очередь, следует обратить внимание на особенности отыскания рассматриваемой информации. Выявленные закономерности такого отыскания свидетельствуют о том, что общеизвестные тактические подходы производства следственных действий не учитывают особенностей доступа к компьютерной информации, сокрытой методами криптографии. Ранее в криминалистике детально не рассматривался вопрос о необходимости формирования именно тактических рекомендаций отыскания, фиксации и исследования информации, преобразованной методами криптографии, с учетом возможного непосредственного или дистанционного противодействия субъекту предварительного расследования со стороны заинтересованных лиц.

Фактически следует говорить о том, что в рамках реализации общетактических задач производства следственных действий в рассматриваемом случае реализуются также и специальные тактические приемы отыскания, фиксации и исследования информации, преобразованной методами криптографии. Эти приемы применяются в процессе изучения данных персональных компьютеров, носителей цифровых данных, серверов, глобальной сети Интернет.

В четвертом параграфе ***«Технико-криминалистическое обеспечение получения компьютерной информации, преобразованной методами криптографии»*** обоснована тактическая необходимость использования аппаратно-программных комплексов для получения

компьютерной информации, преобразованной методами криптографии, не только в рамках судебных экспертиз, но и в ходе проведения отдельных следственных действий. По мнению автора, современные аппаратно-программные комплексы позволяют оперативно выявлять и извлекать компьютерную информацию, что не требует временных затрат и специально созданных условий.

Выбор средств и методов получения и анализа компьютерных данных, преобразованных методами криптографии, зависит от типа технического средства и способов хранения криминалистически значимой компьютерной информации.

Так, в работе подробно исследованы характеристики и особенности получения информации, хранящейся на устройствах сотовой связи. При этом автором предложено пять основных уровней извлечения данных из мобильных устройств:

ручное извлечение данных (обеспечение доступа к компьютерной информации, имеющейся в памяти исследуемого устройства, посредством его клавиатуры или сенсорного экрана);

извлечение данных на логическом уровне (подключение устройства к рабочей станции эксперта посредством USB-кабеля, ИК-порта или Bluetooth);

извлечение данных на физическом уровне (получение побитовой копии всей внутренней памяти исследуемого устройства, что позволяет, в том числе, восстановить удаленные записи и файлы);

извлечение данных из интегральной схемы памяти, или «Chip-off» (извлечение данных непосредственно из интегральной схемы памяти устройства);

извлечение данных на микроуровне.

Автором приведена типология специализированных аппаратно-программных комплексов, внедренных в деятельность отечественных правоохранительных органов, используемых для получения и анализа компьютерной информации, преобразованной методами криптографии. Данные технические средства подразделяются на аппаратные средства, программные средства, аппаратные блокираторы записи, аппаратные средства восстановления данных и программные средства восстановления данных. В работе доказана эффективность использования аппаратно-программных комплексов на основе изученных результатов правоприменительной практики.

В **заключении** акцентируется внимание на основных положениях проведенного исследования; отмечается значимость разработанной комплексной методики обнаружения, фиксации, изъятия и использования субъектами раскрытия и расследования преступлений компьютерной информации, преобразованной методами криптографии.

В **приложениях** содержатся аналитическая справка-обобщение интервьюирования и опроса следователей и оперативных сотрудников органов внутренних дел, участвовавших в расследовании преступлений, связанных с компьютерной информацией, преобразованной методами криптографии; словарь специальных терминов и выражений, используемых в диссертационном исследовании, а также сведения об аппаратно-программных комплексах, предназначенных для выявления и анализа компьютерной информации, преобразованной методами криптографии.

Основные научные результаты диссертации опубликованы в следующих работах автора:

Научные статьи, опубликованные в изданиях, рекомендованных Высшей аттестационной комиссией при Министерстве науки и высшего образования Российской Федерации:

1. Зиновьева Н.С. Алгоритм использования электронного почтового ресурса как источника доказательственной информации / В.И. Еремченко, Н.С. Зиновьева // Вестник Краснодарского университета МВД России. – 2014. – № 3(25). – С. 62–65. – 0,4 п. л. (авторство не разделено).

2. Зиновьева Н.С. Возможности блокчейн-технологии в раскрытии и расследовании преступлений в интернет-пространстве / Н.С. Зиновьева // Вестник Восточно-Сибирского института МВД России. – 2018. – № 3(86). – С. 184–189. – 0,7 п. л.

3. Зиновьева Н.С. К вопросу о месте криптографии и стеганографии в криминалистической науке / Н.С. Зиновьева // Гуманитарные, социально-экономические и общественные науки. – 2019. – № 2. – С. 87–89. – 0,3 п. л.

4. Зиновьева Н.С. Криминалистическое значение диагностики криптографически защищенных объектов / Н.С. Зиновьева // Юристъ-Правоведъ. – 2019. – № 3. – С. 142–146. – 0,6 п. л.

5. Зиновьева Н.С. Использование методов криптографии при производстве, распространении или хранении детской порнографии в информационно-телекоммуникационной системе / Н.С. Зиновьева // Философия права. – 2020. – № 2(93). – С. 120–124. – 0,6 п. л.

Научные статьи, опубликованные в иных изданиях:

6. Зиновьева Н.С. Проблемы использования достижений криминалистической кибернетики в деятельности правоохранительных органов / Н.С. Зиновьева // Проблемы совершенствования законодательства на современном этапе: материалы Междунар. студ. конф., 24 апр. 2014 г. – Белгород: БелЮИ МВД России, 2014. – С. 75–77. – 0,2 п. л.

7. Зиновьева Н.С. Использование кибернетических закономерностей обмена информацией по современным телекоммуникационным системам в антитеррористической деятельности / Н.С. Зиновьева // Актуальные вопросы науки и практики: материалы II Всерос. науч. конф., 17 апр. 2014 г. – Краснодар: Краснодар. ун-т МВД России, 2014. – Т. 1. – С. 237–241. – 0,3 п. л.

8. Зиновьева Н.С. Проблемы использования электронных почтовых ресурсов в раскрытии и расследовании преступлений / В.И. Еремченко, Н.С. Зиновьева // Общественная безопасность, законность и правопорядок в III тысячелетии: сб. материалов Междунар. науч.-практ. конф., 1 окт. 2014 г. – Воронеж: Воронеж. ин-т МВД России, 2014. – Ч. 3. – С. 55–59. – 0,3 п. л. (авторство не разделено).

9. Зиновьева Н.С. Использование современных телекоммуникационных систем как возможность реализации розыскной деятельности следователем / Н.С. Зиновьева // Материалы науч.-практ. конф. молодых ученых / Вост.-Сиб. ин-т Мин-ва внутренних дел Рос. Федерации. – Иркутск, 2014. – С. 37–38. – 0,1 п. л.

10. Зиновьева Н.С. Современные способы противодействия терроризму с использованием информационных технологий / Н.С. Зиновьева // Юридическая наука: история, современность, перспективы: сб. материалов VI Регион. науч.-практ. конф., посвященной Дню российской науки. – М.: Междунар. юрид. ин-т (Астраханский филиал), 2015. – С. 383–387. – 0,3 п. л.

11. Зиновьева Н.С. Проблемы и перспективы использования виртуальных почтовых ресурсов в целях раскрытия и расследования преступления / В.И. Еремченко, Н.С. Зиновьева // Криминалистика и судебно-экспертная деятельность в условиях современности: материалы III Всерос. науч.-практ. конф. – Краснодар: Краснодар. ун-т МВД России, 2015. – С. 162–167. – 0,3 п. л. (авторство не разделено).

12. Зиновьева Н.С. Криминалистическое обеспечение противодействия террористической и экстремистской активности в сети Интернет / В.И. Еремченко, Н.С. Зиновьева // Сб. материалов деловой программы XIX Междунар. выставки средств обеспечения безопасности государства «Интерполитех-2015», 20–23 окт. 2015 г. – М., 2015. – С. 152–153. – 0,1 п. л. (авторство не разделено).

13. Зиновьева Н.С. Закономерности обмена информацией посредством телекоммуникационных систем и их использование в антитеррористической деятельности / Н.С. Зиновьева // Тез. докл. III Междунар. науч.-практ. конф., 20 марта 2015 г. – Могилев: Могилев. ин-т МВД, 2015. – С. 74–75. – 0,1 п. л.

14. Зиновьева Н.С. Возможности раскрытия и расследования преступлений террористической и экстремистской направленности с использованием ресурсов сети Интернет / Н.С. Зиновьева // Актуальные проблемы правоохранительной деятельности глазами молодых ученых: материалы Всерос. науч.-практ. конф. – Симферополь: Краснодар. ун-т МВД России (Крымский филиал), 2016. – С. 36–39. – 0,2 п. л.

15. Зиновьева Н.С. Криминалистическое значение информации, получаемой с электронных носителей / Н.С. Зиновьева // Криминалистика и судебно-экспертная деятельность: теория и практика: материалы V Всерос. науч.-практ. конф. – Краснодар: Краснодар. ун-т МВД России, 2017. – С. 142–144. – 0,2 п. л.

16. Зиновьева Н.С. Криптографические системы защиты информации и их значение в получении криминалистически значимой информации / Н.С. Зиновьева // Криминалистические аспекты процесса доказывания: сб. материалов по результатам Всерос. науч.-практ. конф. – Краснодар: Кубан. гос. ун-т, 2017. – С. 36–38. – 0,2 п. л.

17. Зиновьева Н.С. Учет возможностей блокчейн-технологии в правоохранительной деятельности / Н.С. Зиновьева // Деятельность правоохранительных органов в современных условиях: сб. материалов по результатам XXIII Междунар. науч.-практ. конф. – Иркутск: ФГКОУ ВО ВСИ МВД России, 2018. – Т. 2. – С. 277–278. – 0,1 п. л.

18. Зиновьева Н.С. Криптовалюта как объект криминалистического анализа / Н.С. Зиновьева // Белгородские криминалистические чтения: сб. материалов по результатам Всерос. науч.-практ. конф. – Белгород: ФГКОУ ВО БЮИ МВД России, 2018. – С. 407–410. – 0,2 п. л.

19. Зиновьева Н.С. Алгоритм получения криминалистически значимых сведений, передаваемых посредством блокчейн-технологий /

Н.С. Зиновьева // Криминалистика и судебно-экспертная деятельность: теория и практика: сб. материалов по результатам VI Междунар. науч.-практ. конф. – Краснодар: Краснодар. ун-т МВД России, 2018. – С. 167–170. – 0,2 п. л.

20. Зиновьева Н.С. Криптографическая информация в системе криминалистических знаний / Н.С. Зиновьева // Юридическое образование и наука. – 2019. – № 2. – С. 31–35. – 0,6 п. л.

21. Зиновьева Н.С. Использование криптовалюты при финансировании экстремизма и терроризма / Н.С. Зиновьева // Эффективное противодействие преступности в условия глобализации: проблемы и перспективы: сб. науч. тр. науч.-практ. конф. – Нальчик, 2019. – С. 43–45. – 0,2 п. л.

22. Зиновьева Н.С. Криминалистический анализ информации, сокрытой методами криптографии и стеганографии / Н.С. Зиновьева // Современные проблемы отечественной криминалистики и перспективы ее развития: сб. материалов по результатам Всерос. науч.-практ. конф., посвященной 20-летию кафедры криминалистики Кубанского государственного аграрного университета. – Краснодар: Кубан. гос. аграрный ун-т им. И.Т. Трубилина, 2019. – С. 256–258. – 0,2 п. л.

23. Зиновьева Н.С. О значении профессиональных компетенций сотрудников правоохранительных органов, осуществляющих раскрытие и расследование преступлений в информационно-телекоммуникационной сфере / Н.С. Зиновьева // II Хмыровские криминалистические чтения: сб. материалов по результатам Всерос. науч.-практ. конф. – Краснодар: Кубан. гос. ун-т, 2019. – С. 40–44. – 0,3 п. л.

Иные издания:

24. Зиновьева Н.С. Кибернетика: ее значение и возможности использования в современной деятельности правоохранительных структур: учеб. пособие / В.И. Еремченко, Н.С. Зиновьева. – Краснодар, 2015. – 67 с. – 3,9 п. л. (авторство не разделено).

25. Зиновьева Н.С. Юридические и организационные аспекты использования информационно-телекоммуникационных систем в целях противодействия террористической и экстремистской деятельности в современных условиях / В.И. Еремченко, Н.С. Зиновьева, И.Л. Алексеенко. – Краснодар: Краснодар. ун-т МВД России, 2015. – 67 с. – 3,9 п. л. (авторство не разделено).

Подписано в печать 11.02.2021. Печ. л. 1,5.
Тираж 140 экз. Заказ 118.

Краснодарский университет МВД России.
350005, Краснодар, ул. Ярославская, 128.