А. И. Семикаленова*,
И. А. Рядовский**

Использование специальных знаний при обнаружении и фиксации цифровых следов: анализ современной практики[1]

Аннотация. *В статье проанализированы результаты изучения актуальной практики выявления, фиксации, сохранения и предваряющего судебную экспертизу исследования цифровых следов преступления. В качестве инструментария мониторинга следственной и оперативно-розыскной деятельности в данной области использовались личные беседы и опросы работников Следственного комитета Российской Федерации, следственных и оперативно-розыскных подразделений МВД России, сотрудников иных служб и ведомств, курсантов и студентов старших курсов высших учебных заведений, обучающихся по соответствующей специализации. Кроме того, были опрошены специалисты в области компьютерных информационных технологий как частного, так и государственного сектора, привлекаемые к проведению следственных действий и оперативно-розыскных мероприятий.*

В статье представлены результаты данного исследования, выявлены актуальные проблемы уголовного судопроизводства, с которыми сталкиваются представители правоохранительных органов, расследующие преступления, сопряженные с информационно-компьютерными технологиями, при изъятии и фиксировании компьютерной информации.

Ключевые слова: *информационно-компьютерное обеспечение, компьютерное преступление, следственное действие, обыск, выемка, компьютерная информация, компьютерная сфера, информационно-цифровые технологии, информатизация, цифровые следы, интернет-мошенничества, удаленный доступ, допрос, осмотр, цифровые следы.*

DOI: 10.17803/1994-1471.2019.103.6.178-185

[1] Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-29-16003/18.

* *Семикаленова Анастасия Игоревна*, кандидат юридических наук, доцент кафедры судебных экспертиз Московского государственного юридического университета имени О.Е. Кутафина (МГЮА)
semiks@mail.ru
125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9

** *Рядовский Игорь Анатольевич*, руководитель отдела расследования компьютерных инцидентов АО «Лаборатория Касперского», почетный работник прокуратуры Российской Федерации
igor.ryadovsky@kaspersky.com
125212, Россия, г. Москва, Ленинградское ш., д. 39а, стр. 3

Информационными компьютерными технологиями пронизаны все сферы человеческой деятельности. Было бы странно ожидать, что при широком внедрении компьютеризации в общественные отношения сфера преступной деятельности оказалась бы незатронутой. Сегодня при совершении большого количества преступлений так или иначе используется компьютерное средство[2]: либо в качестве средства совершения преступления, как, например, при осуществлении незаконного доступа к защищаемой информации или интернет-мошенничествах, либо в качестве средства подготовки или сокрытия преступления — лжепредпринимательство, преступления в банковской сфере, распространение наркотических средств и др. Доля таких преступлений с каждым годом неуклонно растет, поэтому для их расследования необходимо существенное углубление и расширение знаний в области компьютерных технологий. Все чаще у следователей и оперативных сотрудников возникает необходимость привлечения лиц, обладающих специальными знаниями в данной области.

Особенно показательным в части распространенности компьютерных технологий (в самом широком смысле) в качестве средств и орудий совершения преступлений стал 2018 г., в течение которого, согласно результатам опросов специалистов по информационной безопасности, впервые доля их участия по делам так называемых традиционных видов преступлений превысила количество дел о преступлениях в сфере компьютерной информации в 1,5 раза. При этом в абсолютных цифрах количество следственных действий и оперативно-розыскных мероприятий по делам о преступлениях в сфере компьютерной информации, в которых участвовали опрошенные специалисты, также возросло. Этот факт подтверждает тезис о всестороннем проникновении информационных технологий в преступную сферу.

В ходе мониторинга следственной и оперативно-розыскной практики проведены опросы и анкетирования специалистов в области IT-технологий, которые показали, что сегодня, помимо участия в расследовании преступлений, сопряженных с неправомерным доступом к компьютерной информации, а также с разработкой и использованием вредоносных программ, указанные специалисты были наиболее востребованы при проведении следственных действий и оперативно-розыскных мероприятий по делам о традиционных видах мошенничества, незаконной организации азартных игр, незаконном обороте наркотических средств, об убийствах, о сообщениях о заведомо ложных актах терроризма. Если проанализировать общее число случаев участия в расследовании преступлений лиц, сведущих в рассматриваемой области знаний, то можно утверждать, что в последнее время возросла потребность следственных органов в дополнительных знаниях.

Особое место в применении специальных компьютерно-технических знаний в следственной и оперативно-розыскной практике занимает обнаружение и фиксация цифровых следов. К указанным следам авторы статьи совместно с профессором Е. Р. Россинской[3] относят криминалистически значимую компьютерную информацию о событиях или действиях, отраженную в материальной среде, в процессе возникновения данной информации, ее обработки, хранения и передачи. Нами в течение последних двух лет было опрошено 100 следователей и 203 оперативных сотрудника. По мнению опрошенных респондентов, независимо от вида расследуемого преступления наиболее значимые мероприятия по обнаружению, сбору и фиксации таких следов связаны с выездами на место: будь

[2] *Чекунов И. Г.* Современные киберугрозы. Уголовно-правовая и криминологическая классификация и квалификация киберпреступлений // Право и кибербезопасность. 2012. № 1. С. 9—22 ; *Нехорошев А. Б.* Компьютерные преступления: квалификация, расследование, экспертиза / под ред. В. Н. Черкасова. Саратов : СЮИ МВД России, 2004. 372 с.

[3] *Россинская Е. Р., Рядовский И. А.* Концепция цифровых следов в криминалистике // Аубакировские чтения : материалы междунар. науч.-практ. конференции (19 февраля 2019 г.). Алматы : Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясының ҒЗжРБЖҰБ, 2019. С. 6—8.

то доступ к рабочей станции подозреваемого в ходе обыска, получение компьютерной техники потерпевших в процессе выемки либо осмотр места происшествия — локальной компьютерной сети. На вопрос, к проведению каких следственных действий они привлекались наиболее часто, специалисты выделили:

— обыск (43 %);
— осмотр места происшествия (31 %);
— осмотр предметов, документов (16 %);
— выемка (10 %).

Федеральным законом от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности»[4] в ст. 6 предусмотрены как специальные мероприятия — снятие информации с технических каналов связи и получение компьютерной информации, так и иные мероприятия, в ходе которых может быть произведен поиск, обнаружение и изъятие цифровых следов преступления. По сведениям, полученным от специалистов в области IT-технологий и оперативных сотрудников МВД России, наиболее часто специалисты привлекались к оперативно-розыскным мероприятиям:

— исследование (36 %);
— снятие информации с технических каналов связи (28 %);
— получение компьютерной информации (17 %);
— сбор образцов для исследования (12 %);
— оперативный эксперимент (7 %).

Анализ анкетных данных и данных опроса сотрудников следственных и оперативно-розыскных подразделений выявил проблему в сборе и фиксации цифровых следов при отображении их на удаленных компьютерных системах. Вызвана данная проблема тем, что уголовно-процессуальным законом не предусмотрены следственные действия по получению компьютерной информации с удаленных компьютерных систем и сетей. В этой связи их приходится разрешать посредством поручения производства таких мероприятий органу, осуществляющему оперативно-розыскную деятельность. Вышеуказанные проблемы возникают при фиксации информации, расположенной на интернет-ресурсах, и часто касаются незаконного оборота наркотических средств, распространения порнографической или иной запрещенной к распространению на территории Российской Федерации информации, лжепредпринимательства.

Хотелось бы отметить, что несмотря на то, что ряд авторов уже писали о необходимости совершенствования действующего законодательства, регламентирующего расследование преступлений в сфере компьютерных технологий[5], а также на то, что законодатель внес в УПК РФ[6] статью 164.1, предусматривающую копирование интересующей следствие информации, все респонденты указывают на несовершенство уголовно-процессуального законодательства в части отсутствия в перечне следственных действий необходимых процессуальных инструментов, в рамках которых возможно удаленное получение компьютерной информации с компьютерных систем и сетей. По мнению респондентов, это особенно важно для расследования компьютерных преступлений, сопряженных с шифрованием информации. Поскольку компьютерные данные очень легко уничтожить либо зашифровать, преступники этим часто пользуются, чтобы скрыть доказательства от следствия. Они уделяют особое внимание мерам конспирации, для чего используют методы шифрования информации с использованием специализированных программных продуктов, типа TrueCrypt. Чтобы получить доступ к такой информации, содержащейся на изъятой копии компьютера, не-

[4] Федеральный закон от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» (в редакции Федерального закона от 6 июля 2016 г. № 374-ФЗ) // СЗ РФ. 2016. № 28. Ст. 4558.

[5] *Торичко Р. С.*, *Клишина Н. Е.* Некоторые вопросы совершенствования действующего законодательства, регламентирующего расследование киберпреступлений // Вестник экономической безопасности. 2018. № 3. С. 179—184.

[6] Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ (ред. от 01.04.2019) // СЗ РФ. 2018. № 53. Ст. 8456.

обходимо ввести пароль либо использовать криптографический ключ, которыми следствие в большинстве случаев не располагает. Другой способ получения доступа к информации, имеющей значение для дела, — произвести удаленное подключение к компьютеру в процессе его работы. Данный способ сегодня может быть реализован только в рамках проведения оперативно-розыскных мероприятий по поручению следователя. Именно поэтому на наш вопрос, каковы главные задачи специалиста при производстве следственных действий и оперативно-розыскных мероприятий, 64 % респондентов ответили, что, помимо оказания содействия в поиске и обнаружении доказательств и применении технических средств, роль специалиста заключается в обеспечении доступа к компьютерным данным, имеющим значение для дела, которые при осмотре электронных носителей информации могут быть в зашифрованном виде.

Проанализировав уголовные дела и результаты опроса следственных и оперативных сотрудников, авторы пришли к выводу, что крайне важно привлекать лиц, обладающих специальными знаниями в области информационно-компьютерных технологий, уже на этапе планирования и подготовки следственных действий, связанных с поиском, обнаружением и фиксацией цифровых следов, — с целью получения компетентных разъяснений относительно доступности электронных доказательств и необходимости принятия мер к их сохранности. Однако обобщение результатов опроса показывает, что, несмотря на признаваемую всеми респондентами значимость данного этапа, наиболее распространенная и, наверное, общая и наиболее значительная ошибка — это отсутствие либо формальный подход к подготовке к проведению следственных действий и оперативно-розыскных мероприятий. Недаром на заведомо провокационный вопрос, каким образом они могли бы описать идеальное следственное действие или оперативно-розыскное мероприятие по сбору цифровых следов преступления, большинство респондентов ответили, что «идеальное мероприятие — это хорошо подготовленное мероприятие».

Из личных бесед с респондентами о показательных примерах из их правоприменительной практики можно сделать вывод, что нередко подготовка не учитывает специфики преступной деятельности в сфере компьютерной информации. Например, ошибка в месте производства обыска, когда квартира либо офис были установлены по входящему в помещение интернет-каналу провайдера, в сетевом трафике которого зафиксированы признаки противоправной активности, без проверки версии о компрометировании Wi-Fi-передатчика лицом, проживающим либо работающим в соседнем помещении. Отсутствие предварительного инструктажа всех участников мероприятия часто приводит к утрате криминалистически значимой информации уже в ходе производства обыска. Следователи и оперативные сотрудники, не имеющие опыта работы по таким делам, не всегда осознают, насколько легко подозреваемый может уничтожить информацию: закрыв крышку ноутбука либо выдернув силовой кабель, что свидетельствует об их недостаточных знаниях в области информационно-компьютерных технологий. Поскольку риск утраты компьютерной информации очень высок (гораздо выше, чем риск утраты традиционных доказательств), необходимо в первую очередь допустить к осмотру вычислительной техники специалистов, знакомых с правилами предосторожности.

В подтверждение такого вывода можно привести показательный пример из следственной практики, обстоятельства которого были изложены одним из респондентов в личной беседе. При подготовке производства обыска в офисном помещении, в котором были оборудованы компьютеризированные рабочие места участников организованной группы, осуществлявшей преступную деятельность в сфере компьютерной информации, следователем был разработан план осмотра и исследования этого помещения. Согласно плану исследование рабочих мест первоначально должен был провести криминалист с целью обнаружения и фиксации следов рук, после чего к осмотру компьютеров допускались специалисты в сфере компьютерной информации. Однако в результате обработки одного из ноутбуков дактилоскопическим порошком

на магнитную кисть среагировал встроенный в корпус датчик закрытия крышки, после чего операционная система переключила компьютер в энергосберегающий режим, следствием чего стала блокировка доступа к информации. Здесь явно прослеживается незнание специалистом-криминалистом особенностей компьютерной техники или элементарное их игнорирование, несоблюдение очередности работы с объектами на месте проведения следственного действия. При более тщательной подготовке обыска, разъяснении всем участникам особенностей работы с компьютерными объектами такого могло не произойти.

Опрос респондентов и личные беседы выявили еще одну проблему использования специальных знаний при поиске и фиксации цифровых следов преступления. Требования действующего законодательства обязывают лицо, производящее в ходе обыска либо выемки обнаружение, фиксацию и изъятие цифровых следов путем изъятия электронных носителей информации и копирования с них информации, привлекать к участию в следственном действии либо оперативно-розыскном мероприятии специалиста (ст. 164.1 УПК РФ). Подавляющее большинство опрошенных сотрудников следственных и оперативно-розыскных подразделений пояснили, что следуют этому требованию путем включения в состав следственно-оперативной группы криминалиста, как правило сотрудника соответствующего подразделения ЭКЦ МВД России, либо привлекают стороннего специалиста в сфере компьютерной техники. Причем, несмотря на отсутствие прямого указания на это в законе, изъятие и копирование электронных носителей информации в ходе осмотра места происшествия проводятся в большинстве случаев также с участием специалиста. Однако все опрошенные следственные и оперативные сотрудники отрицательно ответили на вопрос, понимали ли они, какой именно специализации и компетенции в области информационно-компьютерных технологий специалист им требуется.

В отличие от сотрудников следственных и оперативно-розыскных подразделений, опрошенные в ходе мониторинга специалисты пояснили, что для производства мероприятий, нацеленных на поиск и фиксацию цифровых следов, следует привлекать специалистов, область познаний которых должна быть достаточна широка: в сфере компьютерных устройств и программирования, в области сетевого взаимодействия и эксплуатации сетевой инфраструктуры и т.п., либо следует привлекать нескольких специалистов с углубленными познаниями в определенных областях компьютерно-информационных технологий. При этом привлечение специалиста к проведению следственных действий по уголовным делам о преступлениях в сфере компьютерной информации требует от следователя понимания, каким требованиям должен соответствовать специалист, какими методиками обладать, какие технические средства использовать, чтобы обеспечить исчерпывающие меры к обнаружению и фиксации доказательств и исключить их утрату.

Существенные затруднения при определении источника, содержащего криминалистически значимую информацию, возникают при осмотре крупных компьютерных сетей, функционирование которых приостановить не представляется возможным ввиду непрерывного производственного процесса. Кроме того, изъятие с места происшествия всей компьютерной сети с целью производства судебной экспертизы не является целесообразным и разумным и в большинстве случаев технически возможным. В этом случае перед следователем стоит задача на месте происшествия выявить компьютерные устройства, подлежащие изъятию. При этом ни один из опрошенных представителей правоохранительных органов, за исключением сотрудников специализированных оперативно-розыскных подразделений, не смог ответить, что́ представляют из себя на уровне обработки компьютером перечисленные объекты и процессы операционных систем и как их изучение позволяет выполнить поставленную задачу.

Вместе с тем, как показывают результаты мониторинга, отсутствие даже базовых знаний об устройстве современных компьютеров, о функционировании их сетей, среде и циклах обращения компьютерной информации влияет на качество расследования преступлений,

совершенных с использованием информационно-компьютерных технологий, и может привести к невосполнимой утрате доказательств. Безусловно, привлеченный специалист, обладающий должной компетенцией, обязан оказать профессиональное содействие следователю в поиске и фиксации цифровых следов преступления[7]. Но, как свидетельствуют приведенные выше результаты мониторинга, для привлечения специалиста с соответствующей компетенцией от следователя требуется хотя бы минимальный образовательный уровень в сфере компьютерных технологий и обработки информации.

Одной из проблем сложившегося на сегодняшний день положения дел в следственной практике по поиску и фиксации цифровых следов преступления опрошенные сотрудники следственных и оперативно-розыскных подразделений называют отсутствие должной подготовки привлекаемых к мероприятиям специалистов в части отсутствия у них на месте необходимой криминалистической техники, позволяющей произвести изъятие и фиксацию на носителе-дубликате компьютерной информации в случае невозможности изъятия компьютерной системы, подлежащей исследованию, а в ряде случаев достаточных для проведения данных мероприятий знаний.

В личных беседах специалисты в области IT-технологий подтвердили наличие такой проблемы. Однако подобные ситуации характерны и в случае привлечения специалистов из сторонних, не связанных с обеспечением информационной безопасности организаций. Вместе с тем, по их мнению, обязанность удостовериться в наличии необходимых компетенций привлекаемого специалиста, в том числе выяснить, обладает ли специалист навыками работы с соответствующей криминалистической техникой, а также может ли обеспечить ее применение, лежит на лице, ведущем расследование, что становится невозможным без соответствующих специальных знаний у этого лица.

Опрошенные в ходе мониторинга специалисты также пояснили, что ни один перечень оборудования, инструментов и программного обеспечения, которые могут быть востребованы при изъятии компьютерной техники, обнаружении, осмотре и фиксации компьютерной информации, не может считаться исчерпывающим и должен составляться исходя из конкретных обстоятельств дела. Можно лишь говорить о необходимом минимуме, например:

— программы для снятия снимка (дампа) оперативной памяти (например, Belkasoft RAM Capturer, ProcDump);
— устройства, позволяющие изучать содержимое файловой системы в режиме «только чтение»;
— устройства-блокираторы для копирования НЖМД/SSD, исключающие возможность внесения изменений на исходный диск.

Итак, подводя итоги проведенного мониторинга, можно выделить следующие проблемные ситуации, связанные с поиском, фиксацией и исследованием цифровых следов преступления, приводящие к типичным следственным ошибкам:

— отсутствие подготовительных мероприятий;
— привлечение специалиста, не обладающего необходимой компетенцией;
— нарушение очередности криминалистических методов сбора доказательств, влекущее утрату компьютерной информации, имеющей существенное значение для дела;
— формальный подход к организации следственных действий и оперативно-розыскных мероприятий;
— отсутствие у лиц, проводящих следственные и оперативно-розыскные мероприятия, минимально необходимых знаний в области информационно-компьютерных технологий.

Основной же вывод: отсутствие системного, комплексного подхода в изучении темы расследования компьютерных преступлений в целом и обнаружения и фиксации цифровых следов в частности во многом вытекает

[7] *Чекунов И. Г.*, *Рядовский И. А.*, *Иванов М. А.* [и др.]. Методические рекомендации по расследованию преступлений в сфере компьютерной информации : учебное пособие / под ред. И. Г. Чекунова. М. : Мос. ун-т МВД России имени В. Я. Кикотя, 2018. 106 с.

из недостаточной разработанности темы информационно-компьютерного обеспечения криминалистической деятельности[8], развитие которой в дальнейшем позволит в значительной степени оптимизировать использование человеческих и технических ресурсов с целью быстрого и качественного раскрытия преступлений.

БИБЛИОГРАФИЯ

1. *Нехорошев А. Б.* Компьютерные преступления: квалификация, расследование, экспертиза / под ред. В. Н. Черкасова. — Саратов : СЮИ МВД России, 2004. — 372 с.
2. *Россинская Е. Р.* Концепция частной криминалистической теории «информационно-компьютерное обеспечение криминалистической деятельности» // Деятельность правоохранительных органов в современных условиях : сборник материалов XXIII Международной науч.-практ. конференции : в 2 т. — Иркутск : Восточно-Сибирский институт МВД РФ, 2018. — С. 113—118.
3. *Россинская Е. Р., Рядовский И. А.* Концепция цифровых следов в криминалистике // Аубакировские чтения : материалы международной научно-практической конференции (19 февраля 2019 г.). — Алматы : Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясының ҒЗжРБЖҰБ, 2019. — С. 6—8.
4. *Торичко Р. С.*, *Клишина Н. Е.* Некоторые вопросы совершенствования действующего законодательства, регламентирующего расследование киберпреступлений // Вестник экономической безопасности. — 2018. — № 3. — С. 179—184.
5. *Чекунов И. Г.* Современные киберугрозы. Уголовно-правовая и криминологическая классификация и квалификация киберпреступлений // Право и кибербезопасность. — 2012. — № 1. — С. 9—22.
6. *Чекунов И. Г.*, *Рядовский И. А.*, *Иванов М. А.* [и др.]. Методические рекомендации по расследованию преступлений в сфере компьютерной информации : учебное пособие / под ред. И. Г. Чекунова. — М. : Московский университет МВД России имени В. Я. Кикотя, 2018. — 106 с.

Материал поступил в редакцию 6 мая 2019 г.

[8] *Россинская Е. Р.* Концепция частной криминалистической теории «информационно-компьютерное обеспечение криминалистической деятельности» // Деятельность правоохранительных органов в современных условиях : сборник материалов XXIII Междунар. науч.-практ. конференции : в 2 т. Иркутск : Восточно-Сибирский институт МВД РФ, 2018. С. 113—118.

THE USE OF SPECIAL KNOWLEDGE IN DETECTING AND FIXING DIGITAL TRACES: ANALYSIS OF MODERN PRACTICE[9]

SEMIKALENOVA Anastasia Igorevna, PhD in Law, Associate Professor of the Department of Forensic Examination of the Kutafin Moscow State Law University (MSAL)
semiks@mail.ru
125993, Russia, Moscow, ul. Sadovaya-Kudrinskaya, d. 9

RYADOVSKIY Igor Anatolievich, Head of Computer Investigation Department, Kaspersky Lab JSC, Honorary Prosecutor of the Russian Federation
igor.ryadovsky@kaspersky.com
125212, Russia, Moscow, Leningradskoye Shosse, d. 39a, str. 3

Abstract. *The paper analyzes the results of studying the current practice of identifying, fixing, preserving and anticipating the forensic examination of the study of digital traces of crime. As a toolkit for monitoring investigative and operational investigative activities in this area, there were applied personal conversations and surveys of employees of the Investigative Committee of the Russian Federation, investigative and operational search units of the Ministry of the Interior of Russia, employees of other services and departments, students of the relevant specialization. In addition, experts in the field of computer information technologies from both the private and public sector, involved in investigative actions and operational search activities were interviewed.*
The paper presents the results of this study, identifying current problems of criminal justice, faced by law enforcement officials investigating crimes involving information and computer technology, while seizing and recording computer information.

Keywords: *information and computer software, computer crime, investigative action, search, seizure, computer information, computer sphere, information digital technologies, informatization, digital traces, Internet fraud, remote access, interrogation, inspection, digital traces.*

REFERENCES (TRANSLITERATION)

1. Nekhoroshev A. B. Komp'yuternye prestupleniya: kvalifikaciya, rassledovanie, ekspertiza / pod red. V. N. Cherkasova. — Saratov : SYuI MVD Rossii, 2004. — 372 s.
2. Rossinskaya E. R. Koncepciya chastnoj kriminalisticheskoj teorii «informacionno-komp'yuternoe obespechenie kriminalisticheskoj deyatel'nosti» // Deyatel'nost' pravoohranitel'nyh organov v sovremennyh usloviyah : sbornik materialov XXIII Mezhdunarodnoj nauch.-prakt. konferencii : v 2 t. — Irkutsk : Vostochno-Sibirskij institut MVD RF, 2018. — S. 113—118.
3. Rossinskaya E. R., Ryadovskij I. A. Koncepciya cifrovyh sledov v kriminalistike // Aubakirovskie chteniya : materialy mezhdunarodnoj nauchno-prakticheskoj konferencii (19 fevralya 2019 g.). — Almaty : Қazaқstan Respublikasy IIM M. Esbolatov atyndaғy Almaty akademiyasynyң ҒZzhRBZh¥B, 2019. — S. 6—8.
4. Torichko R. S., Klishina N. E. Nekotorye voprosy sovershenstvovaniya dejstvuyushchego zakonodatel'stva, reglamentiruyushchego rassledovanie kiberprestuplenij // Vestnik ekonomicheskoj bezopasnosti. — 2018. — № 3. — C. 179—184.
5. Chekunov I. G. Sovremennye kiberugrozy. Ugolovno pravovaya i kriminologicheskaya klassifikaciya i kvalifikaciya kiberprestuplenij // Pravo i kiberbezopasnost'. — 2012. — № 1. — S. 9—22.
6. Chekunov I. G., Ryadovskij I. A., Ivanov M. A. [i dr.]. Metodicheskie rekomendacii po rassledovaniyu prestuplenij v sfere komp'yuternoj informacii : uchebnoe posobie / pod red. I. G. Chekunova. — M. : Moskovskij universitet MVD Rossii imeni V. Ya. Kikotya, 2018. — 106 s.

[9] The study is carried out with the financial support of the Russian Foundation for Basic Research, Research Project No. 18- 29- 16003/18.