УДК 343.985
DOI 10.52452/19931778_2021_5_149

ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ ЦИФРОВЫХ СРЕДСТВ ДОКАЗЫВАНИЯ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

А.Г. Холевчук, А.В. Савченко

Кубанский государственный университет, Новороссийск

aholevchuk@mail.ru

Поступила в редакцию 01.04.2020

Исследуются особенности использования цифровых доказательств в процессе расследования преступлений. Рассматриваются вопросы становления и развития цифровой криминалистики, имеющей непосредственное отношение к сбору и анализу электронных доказательств. Определены некоторые проблемы в области цифровой криминалистики. Раскрыты особенности хранения пользовательских данных на различных устройствах (Amazon Echo; iPhone Health), а также основные пробелы в уголовно-процессуальном законодательстве Российской Федерации, связанные с производством отдельных следственных действий. Представлены результаты Доклада (УНП ООН) о работе Группы экспертов для проведения системного исследования проблем компьютерной преступности (2019 г.).

Ключевые слова: цифровая криминалистика; информационные технологии; цифровые следы; цифровые устройства; цифровые доказательства; информационная безопасность; запоминающие устройства; компьютерная информация; компьютерные технологии; электронные доказательства.

В криминалистической науке исторически установлен порядок документирования и обработки информации с последующим использованием ее в качестве доказательств по уголовному делу. С активным развитием информационных технологий возникла необходимость в получении цифровых доказательств в производстве по уголовным делам [1].

В настоящий момент цифровая криминалистика является важнейшим инструментом, способствующим расследованию преступлений, совершенных с помощью компьютерных технологий, в том числе при расследовании иных преступлений, доказательства которых могут храниться в памяти цифровых устройств. Важнейшую роль в обеспечении информационной безопасности играют инструменты цифровой криминалистики, посредством которых восстанавливаются доказательства, оставленные в процессе различных кибератак [2].

То, что мы привыкли понимать под криминалистическими методами, разрабатывалось в первую очередь для восстановления утерянных или испорченных данных. Уже к концу 1980-х годов распространились различные программные приложения, выполняющие функции восстановления цифровых данных (Unformat, Undelete, Diagnose&Remedy и т.д.).

1999–2007 годы стали «золотым веком» цифровой криминалистики. В этот период цифровая криминалистика смогла взглянуть в прошлое путем восстановления остаточных данных, которые, как считалось, были удалены, путем восстановления электронной почты и содержащихся в ней сообщений. Экспертизы сети и памяти позволили наблюдать за этапами совершения преступлений даже спустя долгие месяцы после самого их факта. Этот период развития цифровой криминалистики охарактеризовался широким развитием научных исследований по всему миру [3; 4].

В настоящее время большая часть прогресса цифровой криминалистики последнего десятилетия становится менее актуальной. Полученные в процессе исследований результаты и достижения в данной области находятся на грани потери. Связано это с достижениями и фундаментальными изменениями, происходящими в области развития информационно-коммуникационных технологий. В настоящее время цифровая криминалистика сталкивается со следующими проблемами.

1. Растет количество запоминающих устройств, а это означает, что в большинстве случаев специалисты сталкиваются с нехваткой времени для создания криминалистического изображения предметного устройства или обработки всех обнаруженных данных.

2. Возрастает распространение аппаратных интерфейсов, что приводит к отсутствию относительно легкой возможности удаления и отображения с устройств хранения.

3. Распространенность операционных систем и форматов файлов, в том числе и создание новых, приводит к необходимости совершенствования имеющихся инструментов получения и

последующего использования данных, а разработка новых инструментов требует, как правило, существенных финансовых затрат.

4. Если ранее случаи ограничивались лишь исследованием одного устройства, сейчас чаще возникает необходимость исследования сразу нескольких с последующим соотношением полученных доказательств, что зачастую бывает достаточно проблематично организовать по различным причинам.

5. Широкое распространение шифрования данных приводит к тому, что даже в тех случаях, когда эти данные подлежат восстановлению, их обработка зачастую не представляется возможной.

6. Вредоносные программы, не записываемые в постоянное хранилище, требуют дорогостоящей экспертизы оперативной памяти [5; 6].

Сейчас в основе цифровой криминалистики лежит принцип обмена, сформулированный Эдмоном Локаром, который был убежден, что каждый контакт объекта с поверхностью оставляет след. В контексте цифровой криминалистики это означает, что человек после использования информационно-коммуникационных технологий оставляет цифровые следы. Таким образом, лицо, использующее информационно-коммуникационные технологии, оставляет свои цифровые следы, информацию о возрасте, поле, геолокации, расовой и национальной принадлежности, семейном положении, данных банковских карт и т.д. Подобные цифровые следы могут быть активными или пассивными [7]. Активные создаются данными, которые предоставляют пользователи (персональные данные, видео, изображения, а также комментарии, оставляемые пользователями на различных сайтах). Пассивными цифровыми следами являются те, что умышленно оставлены лицом, пользующимся сетью Интернет и цифровыми технологиями (история просмотров в браузере). Данные активных и пассивных следов могут использоваться в качестве доказательств совершения преступления. Они могут использоваться в качестве доказательств или же опровержения определенной информации о факте; подтверждения или опровержения показаний потерпевшего, свидетеля или подозреваемого, в том числе и при определении причастности (непричастности) подозреваемого к совершению преступления [8; 9].

Данные, полученные в режиме «онлайн» из цифровых устройств, зачастую содержат относительно большое количество криминалистически значимой информации о пользователях и событиях, связанных с преступлением. Например, некоторые игровые приставки хранят конфиденциальную информацию о личности владельца. Стоит отметить, что данные, извлекаемые из игровых приставок, использовались при раскрытии преступлений, связанных с сексуальной эксплуатацией детей, в том числе с размещением в сети Интернет материалов, демонстрирующих сцены сексуального насилия. Еще одним устройством, накапливающим значительный объем личных данных о пользователе, является Amazon Echo с голосовым помощником Alexa. Данные, хранящиеся на этом устройстве, содержат значимые сведения о его пользователе (интересы, предпочтения, совершаемые покупки, геопозиция). Отмечается, что данные, извлеченные из устройства, ранее использовались в США при расследовании дел об убийствах. Обвинения против подозреваемого были сняты, однако сведения, полученные с помощью современных цифровых технологий, были представлены в суде в качестве доказательств [10].

Особый интерес представляет приложение iPhone Health («Здоровье»), собирающее данные пользователя о повседневной деятельности. Подробные данные о пройденных шагах и расстоянии хранятся в базе данных вместе с информацией о времени, с точностью до нескольких минут. Полагаем, что подобная информация будет весьма ценной в расследовании преступлений. С криминалистической точки зрения, данные активности пользователя могут представлять значимую информацию. Например, вероятность прохождения лицом определенного маршрута. В данном случае, если имеются несколько вариантов возможных маршрутов, которые могли быть пройдены конкретным лицом, возможно сопоставить данные маршруты со следами, сохранившимися в приложении iPhone Health («Здоровье»). Исходя из сопоставления вероятных маршрутов с данными приложения, можно предположить, что один из маршрутов был пройден конкретным лицом. Аналогичным образом можно оценить соответствующие временные периоды, в которые пользователь устройства был активен. Тот факт, что данные, полученные в приложениях, собирающих информацию о здоровье пользователя, представляют собой ценную информацию, не остался незамеченным в правоохранительных органах. В Нидерландах данные, полученные из iPhone Health («Здоровье»), использовались в качестве доказательств при расследовании различных преступлений. Несмотря на то что эти данные являются ценным источником информации в уголовном судопроизводстве, необходимо располагать точными сведениями об их достоверности, что и было предпринято в исследовании,

проведенном Нидерландским институтом судебных экспертиз. Результаты подтвердили возможность использования правоохранительными органами данных из приложения iPhone Health («Здоровье») [11].

Отметим, что данные могут быть добыты и использованы с целью получения оперативно-разыскной информации или могут быть представлены в суде в качестве цифровых доказательств. В последнем случае цифровые доказательства могут являться прямыми доказательствами путем установления факта. Могут являться также и косвенными, но уже путем выведения заключения об истинности данного факта. Например, материалы оскорбительного содержания были опубликованы от имени учетной записи (А.) в Twitter. Прямым доказательством в данном случае будет являться факт того, что учетная запись (А.) была непосредственно использована для публикации оскорбительного материала. Косвенным доказательством будет являться факт того, что данный материал был размещен пользователем данной записи (А.) [12; 13].

В сравнении с традиционными доказательствами цифровые создают определенные сложности в аутентификации, что связано с объемом доступных данных, со скоростью их передачи, с их неустойчивостью, которая проявляется в их удалении или перезаписи, а также с тем, что их можно легко повредить или изменить. В то время как одни государства вводят в законодательство нормы доказательственного права, включающие основные требования аутентификации, относящиеся к цифровым доказательствам, другие для аутентификации вещественных и цифровых доказательств используют иной подход [14; 15].

В Российской Федерации получение и анализ доказательств по делам о преступлениях в сфере компьютерной информации является одной из самых основных и трудно разрешаемых задач на практике. Решение этой задачи требует не только разработки тактики производства отдельных следственных действий, но и наличия специальных знаний в области информационных технологий и специального программного обеспечения, а также внесения соответствующих поправок в действующее законодательство.

В связи с тем, что цифровая информация не воспринимается человеком, он, в свою очередь, не может выступать первичным ее носителем. Следовательно, получить цифровую информацию посредством проведения очной ставки, осмотра, допроса или освидетельствования не представляется возможным. Тем не менее в отечественной процессуальной литературе не раз высказывалось мнение, что сбор цифровой информации возможен посредством проведения осмотра. С.П. Кушниренко и Е.И. Панфиловой высказано мнение о том, что информация, хранящаяся на компьютере или съемном носителе, может быть использована в качестве доказательственной путем ее осмотра с помощью аналоговых составляющих компьютера (монитора) [16; 17].

Так, Л.Б. Краснова, говоря о необходимости осмотра цифровой информации, ссылалась на то, что в ходе следствия зачастую возникают ситуации, когда есть данные о том, что на техническом устройстве содержится информация, способствующая эффективному осмотру, это могут быть определенные схемы и чертежи, карты, коды доступа и т.д., и эту информацию необходимо получить в кратчайший срок. Развила данную мысль и Б. Толеубекова, отметившая, что результаты осмотра электронной информации могут существенным образом повлиять на дальнейший процесс расследования преступления. Процессуально значимым последствием может стать основание для назначения судебной экспертизы [18; 19].

Несмотря на различные мнения относительно производства отдельных следственных действий с целью получения цифровых доказательств, в настоящее время единственным методом, предусмотренным законодательством, является собирание цифровой информации путем производства таких следственных действий, как обыск, выемка, контроль и запись переговоров, а также проведение экспертизы. Производятся и иные процессуальные действия, включающие в себя направление запросов в различные органы и организации. Так, американской компанией IBM осуществляется помощь правоохранительным органам в области расследования преступлений в сфере компьютерной информации путем предоставления унифицированной информации о преступлениях и их профессиональной оценке. Программные продукты, разработанные данной компанией, оказывают помощь в расследовании преступлений, сокращая время обработки данных. Компания предоставляет аналитические материалы и рекомендации правоохранительным органам для максимально полезного использования программного обеспечения [20]. Стоит отметить, что в России подобную работу осуществляет компания IB-Group, сотрудники которой принимают участие в следственных действиях по инициативе органов внутренних дел, проводят различные виды сложных компьютерно-технических экспертиз.

Отметим, что перечень обстоятельств, для установления которых обязательно необходимо проведение судебной экспертизы, является ис-

черпывающим. Однако для раскрытия преступлений в сфере компьютерной информации в обязательном порядке необходимо исследование вопросов, связанных с заведомым предназначением компьютерной программы или иной цифровой информации с целью намеренного уничтожения, блокирования, изменения или копирования цифровой информации, а также нейтрализации средств ее защиты. В связи с этим представляется необходимым дополнить ч. 1 ст. 196 УПК РФ пунктом «6», который бы содержал необходимость производства данной экспертизы [21; 22].

Следует отметить, что действующий Уголовно-процессуальный кодекс РФ многие вопросы оставляет неурегулированными. На практике отмечаются ситуации, когда доступ к материальному носителю значимой для дела информации является затруднительным или невозможным.

Открытым вопросом в настоящее время остается процессуальное закрепление нового вида доказательств, а именно «электронных доказательств». Несмотря на распространенность термина «электронное доказательство», многие исследователи убеждены, что выделять данный вид доказательства в качестве самостоятельного и тем более закреплять его в уголовно-процессуальном законе нет необходимости. Р.И. Оконенко в своем диссертационном исследовании, посвященном электронным доказательствам, пришел к выводу, что в настоящее время говорить об электронных доказательствах как о сформировавшейся категории позитивного права пока не стоит, а введение в Уголовно-процессуальный кодекс РФ термина «электронный носитель информации» необходимо рассматривать как первый шаг к появлению в отечественном законодательстве термина «электронные доказательства». Р.И. Оконенко убежден, что электронные доказательства не представляют собой особого вида. Иной точки зрения придерживается А.В. Кудрявцева, полагая, что компьютерную информацию необходимо выделять в качестве самостоятельного вида доказательств [23].

Длительное время открытым оставался вопрос о природе цифровых доказательств, в том числе о том, как они отличаются от характеристик вещественных доказательств. На наш взгляд, вопрос об определении понятия электронных доказательств необходимо решать в каждом конкретном случае, соблюдая при этом нормы национального уголовно-процессуального законодательства.

В заключение отметим результаты встречи представителей ряда государств в Австрии (г. Вена), целью которой являлось обсуждение ключевых вопросов Доклада о работе совещания Группы экспертов для проведения системного исследования проблем компьютерной преступности. По итогам обсуждений была отмечена проблема отсутствия на международном уровне единого определения электронных доказательств. Другим значимым вопросом стало закрепление возможности предоставления правоохранительным органам полномочий на сбор электронных доказательств с соблюдением конфиденциальности, в том числе неприкосновенности частной жизни и прав человека, вместе с предоставлением определенных правовых гарантий [24; 25].

Результаты встречи можно представить следующими ключевыми выводами.

1. Активное создание программных средств и приложений со встроенным шифрованием значительно усложняет доступ к необходимым данным, которые могли бы использоваться в качестве электронных доказательств в отсутствие ключей дешифрования.

2. Применение при расследовании преступлений искусственного интеллекта, в частности при распознавании лиц и преступлений, связанных с нарушением авторских прав, позволяет эффективно использовать ресурсы и время при изучении больших объемов данных и поиске электронных доказательств.

3. Определенные трудности вызывает соотнесение сведений с определенным абонентом по IP-адресу. Дело в том, что у поставщиков интернет-услуг есть возможность присвоить один IP-адрес сразу нескольким абонентам. В связи с этим возникла необходимость в точном определении абонента, которому присвоен конкретный IP-адрес в определенный момент времени.

4. Недостаточность технико-криминалистических средств и оборудования, которое зачастую оказывается дорогостоящим, ограниченность ресурсов криминалистической экспертизы и трудности, связанные с набором квалифицированных специалистов, усложняют процесс получения электронных доказательств [26].

Таким образом, развитие и распространение технологий, преобразовывающих обычную информацию в цифровую, приводит к необходимости совершенствования криминалистических средств и методов, используемых в процессе расследования компьютерных преступлений. Использование электронных доказательств в расследовании является перспективным направлением не только процессуальной, но и криминалистической деятельности. Проблема совершенствования законодательства заключается во внесении необходимых изменений, поскольку цифровые технологии дают значительные возможности для эффективного раскрытия и расследования преступлений.

Список литературы

1. Овчинникова О.В. Проблемы собирания электронных доказательств стороной защиты // Вестник ЮУрГУ. Серия: Право. 2018. № 3. С. 27–33.

2. Русанова Д.Ю. Цифровая криминалистика: возможности и перспективы развития // Международный журнал гуманитарных и естественных наук. 2019. № 12-4. С. 142–145.

3. Garfinkel S.L. Digital forensics research: The next 10 years // Digital Investigation. 2010. № 7. P. 64–73.

4. Cerezo A.I., Lopez J., Patel A. International cooperation to fight transnational cybercrime // In: Second International Workshop on Digital Forensics and Incident Analysis (WDFIA 2007); August 27–28 2007. P. 13–27.

5. Комаров И.М. «Цифровая» криминалистика в актуальных тезисах // Правовая мысль в образовании, науке и практике. 2018. № 4. С. 48–51.

6. Степаненко Д.А., Коломинов В.В. Цифровая реальность и криминалистика // ГлаголЪ правосудия. 2018. № 3 (17). С. 38–43.

7. Servida F., Casey E. IoT forensic challenges and opportunities for digital traces // Digital Investigation. 2019. № 28. P. 22–29.

8. Петров С.В. Цифровые (виртуальные) следы как новое направление исследований в криминалистике // Современные научные исследования и разработки. 2018. № 12. С. 685–687.

9. Лушин Е.А. О термине «электронно-цифровые следы» // Расследование преступлений: проблемы и пути их решения. 2017. № 4. С. 161–163.

10. Casey E. Trust in digital evidence // Forensic Science International: Digital Investigation. 2019. № 31. P. 1–2.

11. Zandwijk J.P., Bostaz A. The iPhone Health App from a forensic perspective: can steps and distances registered during walking and running be used as digital evidence // Digital Investigation. 2019. № 28. P. 126–133.

12. Рудакова С.В. Цифровое алиби и цифровые доказательства // Юридический вестник Кубанского государственного университета. 2019. № 1. С. 56–59.

13. Новицкий В.А., Новицкая Л.Ю. Понятие цифровых доказательств // Ленинградский юридический журнал. 2019. № 1. С. 213–221.

14. Олиндер Н.В. К вопросу о доказательствах, содержащих цифровую информацию // Юридический вестник Самарского университета. 2017. № 3. С. 23–27.

15. Журкина О.В. Доказательства в уголовно-процессуальном законодательстве зарубежных стран // Вопросы российского и международного права. 2016. № 3. С. 109–116.

16. Воронин М.И. Электронные доказательства в УПК: быть или не быть? // Lex Russia. 2019. № 7. С. 75–83.

17. Кушниренко С.П., Панфилова Е.И. Уголовно-процессуальные способы изъятия компьютерной информации по делам об экономических преступлениях: Учебное пособие. СПб., 2003.

18. Краснова Л.Б. Электронные носители информации как вещественные доказательства // Известия Тульского государственного университета. Экономические и юридические науки. 2013. № 4-2. С. 254–260.

19. Толеубекова Б. Компьютерные преступления доказать сложно // Зангер. 2005. № 11. С. 35–36.

20. Гаврилин Ю.В. Электронные носители информации в уголовном судопроизводстве // Труды Академии управления МВД России. 2017. № 44. С. 47–48.

21. Островский О.А. Значение цифровых доказательств при расследовании уголовных преступлений // Вестник Российского университета дружбы народов. 2019. № 1. С. 123–140.

22. Назаров С.В. Об обеспечении достоверности доказательств в «цифровом правосудии» // Дневник науки. 2018. № 6. С. 26.

23. Оконенко Р.И. «Электронные доказательства» и проблемы обеспечения прав граждан на защиту тайны личной жизни в уголовном процессе: сравнительный анализ законодательства США и РФ: Дис. …канд. юрид. наук. М., 2016.

24. Никитина Е.В. Некоторые вопросы собирания электронно-цифровых доказательств // Технологии XXI века в юриспруденции: Материалы Всероссийской научно-практической конференции / Под ред. Д.В. Бахтеева. 2019. С. 103–107.

25. Ширяев А.А. О современных технологиях в расследовании преступлений: компьютерная криминалистика // Общетеоретические и отраслевые проблемы науки и пути их решения: Сб. статей по итогам Международной научно-практической конференции / Отв. ред. А.А. Сукиасян. 2019. С. 210–211.

26. Седова Д.А. Философия трансформации доказывания в условиях развития новых технологий: Международный аспект // Российский журнал правовых исследований. 2019. № 2. С. 112–118.

PROBLEMS OF USING DIGITAL EVIDENCE IN THE INVESTIGATION OF CRIMES IN THE FIELD OF COMPUTER INFORMATION

A.G. Holevchuk, A.V. Savchenko

The article examines the features of using digital evidence in the process of crime investigation. The article deals with the formation and development of digital criminology, which is directly related to the collection and analysis of electronic evidence. Some problems in the field of digital criminology have been identified. Features of storing user data on various devices (Amazon Echo; iPhone Health), as well as the main gaps in the criminal procedure legislation of the Russian Federation related to the production of individual investigative actions are disclosed. The results of the Report (UNODC) on the work of the expert Group for conducting a systematic study of computer crime problems (2019) are presented.

Keywords: digital forensics; information technology; digital tracks; digital devices; digital evidence; information security; storage devices; computer information; computer techologies; electronic evidence.

References

1. Ovchinnikova O.V. Problems of collecting electronic evidence by the defense party // Bulletin of SUSU, series «Law». 2018. № 3. P. 27–33.

2. Rusanova D.Yu. Digital criminalistics: opportunities and prospects for development // International journal of humanities and natural sciences. 2019. № 12-4. P. 142–145.

3. Garfinkel S.L. Digital forensics research: The next 10 years // Digital investigation. 2010. № 7. P. 64–73.

4. Cerezo A.I., Lopez J., Patel A. International cooperation to fight transnational cybercrime // In: Second international workshop on digital forensics and incident analysis (WDFIA 2007); August 27–28. 2007. P. 13–27.

5. Komarov I.M. «Digital» criminalistics in actual theses // Legal thought in education, science and practice. 2018. № 4. P. 48–51.

6. Stepanenko D.A., Kolominov V.V. Digital reality and criminology // Verb justice. 2018. № 3 (17). P. 38–43.

7. Servida F., Casey E. IoT forensic challenges and opportunities for digital traces // Digital investigation. 2019. № 28. P. 22–29.

8. Petrov S.V. Digital (virtual) traces as a new direction of research in criminology // Modern scientific research and development. 2018. № 12. P. 685–687.

9. Lushin E.A. About the term «electronic digital traces» // Investigation of crimes: problems and ways to solve them. 2017. № 4. P. 161–163.

10. Casey E. Trust in digital evidence // Forensic Science International: Digital Investigation. 2019. № 31. P. 1–2.

11. Zandwijk J.P., Bostaz A. The iPhone Health App from a forensic perspective: can steps and distances registered during walking and running be used as digital evidence? // Digital investigation. 2019. № 28. P. 126–133.

12. Rudakova S.V. Digital alibi and digital evidence // Legal Bulletin of the Kuban State University. 2019. № 1. P. 56–59.

13. Novitsky V.A., Novitskaya L.Yu. The concept of digital evidence // Leningrad legal journal. 2019. № 1. P. 213–221.

14. Olinder N.V. On the issue of evidence containing digital information // Legal Bulletin of Samara University. 2017. № 3. P. 23–27.

15. Zhurkina O.V. Proofs in criminal procedure legislation of foreign countries // Questions of Russian and international law. 2016. № 3. P. 109–116.

16. Voronin M.I. Electronic evidence in the criminal procedure code: to be or not to be? // Lex Russia. 2019. № 7. P. 75–83.

17. Kushnirenko S.P., Panfilova E.I. Criminal procedure methods for removing computer information in cases of economic crimes: textbook. SPb., 2003.

18. Krasnova L.B. Electronic media as evidence // Bulletin Tula State University. Economic and legal Sciences. 2013. № 4-2. P. 254–260.

19. Toleubekova B. Computer crimes are difficult to prove // Sanger. 2005. № 11. P. 35–36.

20. Gavrilin Yu.V. Electronic media in criminal proceedings // Proceedings of the Academy of management of the Ministry of Internal Affairs of Russia. 2017. № 44. P. 47–48.

21. Ostrovsky O.A. The value of digital evidence in the investigation of criminal offenses // Bulletin of the Russian University of Peoples' Friendship. 2019. № 1. P. 123–140.

22. Nazarov S.V. On ensuring the reliability of evidence in «digital justice» // Journal of science. 2018. № 6. P. 26.

23. Okonenko R.I. «Electronic evidence» and problems of ensuring the rights of citizens to protect privacy in criminal proceedings: comparative analysis of the legislation of the USA and the Russian Federation: Dissertation of the Candidate of Legal Sciences. M., 2016.

24. Nikitina E.V. Some questions of collecting electronic and digital evidence // Technologies of the XXI century in jurisprudence. 2019. P. 103–107.

25. Shiryaev A.A. On modern technologies in crime investigation: computer criminalistics // General theoretical and branch problems of science and ways of their solution. 2019. P. 210–211.

26. Sedova D.A. Philosophy of transformation of evidence in the conditions of development of new technologies: international aspect // Russian journal of legal research. 2019. № 2. P. 112–118.