УДК 340.68 DOI: 10.18698/2541-8009-2019-05-473

МЕТОДИЧЕСКИЕ ОСНОВЫ ИССЛЕДОВАНИЯ ПРЕДПОЛОЖИТЕЛЬНО ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ В РАМКАХ СУДЕБНОЙ КОМПЬЮТЕРНО-ТЕХНИЧЕСКОЙ ЭКСПЕРТИЗЫ

А.А. Баюш annabayush@mail.ru
SPIN-код: 3271-9054

МГТУ им. Н.Э. Баумана, Москва, Российская Федерация

Аннотация

Рассмотрены основные методические рекомендации по изучению предположительно вредоносного программного обеспечения в рамках судебной компьютерно-технической экспертизы (СКТЭ), назначенной уполномоченными органами и должностными лицами. Определен метод экспертного исследования, даны методические основы (рекомендации) исследования в целом, проведена параллель между понятиями «вирус» и «вредоносная программа». Представлена общая классификация современных вредоносных программ и выполнен их общий анализ. Описан алгоритм производства СКТЭ при изучении вредоносного программного обеспечения в целом и его свойств в отдельности как объекта исследования данной судебной экспертизы.

Ключевые слова

Судебная экспертиза, судебный эксперт, заключение эксперта, специальные знания, судебная компьютерно-техническая экспертиза (СКТЭ), вредоносные программы (вредоносное программное обеспечение), классификация вредоносных программ

Поступила в редакцию 04.04.2019

Актуальность настоящей статьи обусловлена повсеместным внедрением информационных (компьютерных) технологий почти во все сферы человеческой жизнедеятельности. Кроме того, в результате появления огромного количества электронных средств неукоснительно растет объем оставляемых ими информационных следов как в сети Интернет, так и вне ее пределов. Поиск этих следов является основной задачей судебной компьютерно-технической экспертизы. Широко распространились новые — компьютерные — преступления, латентные (скрытные) и очень специфичные по своему характеру, поскольку их основные следы, существующие в виртуальном пространстве, являются недоступными для непосредственного представления участникам судопроизводства без применения специальных программно-технических средств. Раскрытие и расследование таких преступлений представляется невозможным без использования специальных знаний из области информационных технологий, носителем которых является сам судебный эксперт, прошедший соответствующую подготовку в области СКТЭ.

Для эффективного расследования конкретного дела, в рамках которого была назначена судебная экспертиза, необходимо провести комплексное исследование объектов, представленных на экспертизу и имеющих доказательственное

значение по данному делу, которое должно быть основано на определенном алгоритме действий с учетом специфики проведения конкретного вида и отдельных обстоятельств расследуемого дела. Так, различными государственными учреждениями и иными экспертными организациями (например, частными лабораториями, союзами экспертных организаций и др.) разработаны отдельные методические рекомендации (методики) и методические пособия, в которых прописывается алгоритм действий, необходимых для получения определенного результата. Такие методики представляют собой регламентированную, прописанную в соответствующих источниках совокупность действий без теоретических разъяснений, применяемую в целях достижения определенной практической цели исследования. Применение таких действий в большинстве случаев влечет за собой заранее определенный результат, что положительным образом сказывается на качестве выводов составленного судебным экспертом заключения эксперта.

Прежде всего автор считает нужным акцентировать внимание непосредственно на самом понятии «метод». Метод в общеизвестном толковании обозначает некий способ, направленный на достижение поставленной цели, применяемый на практике в процессе реализации определенного рода деятельности с учетом его конкретных обстоятельств и характерных черт; с философской (гносеологической) точки зрения он является ключевым аспектом в процессе познания окружающей действительности [1, с. 230]. Само понятие «метод» пришло из греческого языка и переводится как «путь исследования». Метод в науке в целом подразумевает некий способ как практического, так и теоретического изучения объекта, основанный на знании закономерностей и особенностей последнего. Метод экспертного исследования представляет собой систему логических и инструментальных (либо только логических или только инструментальных) операций поиска и сбора данных для решения вопросов, поставленных перед судебным экспертом. Операции, входящие в состав какого-либо метода, реализуют практическое применение знаний о закономерностях объективной действительности на практике для получения новых знаний об исследуемом объекте, представленном на экспертизу [2, с. 82]. Совокупность таких экспертных методов исследования в соответствии с определенной закономерностью и очередностью выполнения представляет собой непосредственно методические основы (рекомендации) исследования определенных объектов судебной экспертизы конкретного вида.

В современных условиях жизни многие компьютерные технологии и информационные системы разработаны и функционируют для передачи данных, а именно для обмена необходимой информацией между пользователями. Еще до появления сети Интернет и иных сетей была создана система обмена данными и различным программным обеспечением непосредственно между пользователями (например, передача информации с использованием гибких магнитных дисков и т. п.), однако такой обмен данными может нести в себе немалую угрозу — распространение вредоносных программ и заражение ими.

Перед судебными экспертами в области СКТЭ часто ставятся задачи по нахождению (поиску) каких-либо вирусов, т. е. они отвечают на вопросы о наличии либо отсутствии вредоносных программ в определенном программном обеспечении. Необходимо обратить внимание, что в уголовном праве нет понятия «вирус», а установлено такое понятие, как «вредоносные программы» [3, ст. 273], поскольку кроме так называемых вирусов существуют вредоносные программы, осуществляющие простой мониторинг за действиями пользователя, перехват интересующей злоумышленников информации и др. Часто лица, назначающие и запрашивающие экспертизы, не понимают такого различия данных понятий, из-за чего и возникают противоречия. Согласно ГОСТ Р 57429–2017 «Судебная компьютерно-техническая экспертиза. Термины и определения», компьютерный вирус (*Computer virus, Virus*) — это программа, способная к самостоятельному распространению по локальным сетям, средствам вычислительной техники, не использующая сетевые сервисы [4, п. 1.1].

Под вредоносными программами (также деструктивными программами) принято понимать программы, направленные на реализацию несанкционированного доступа, в процессе которого возможно осуществление копирования, видоизменения, уничтожения либо блокировки данных, а также вызывающие сбои функционирования в работе различных программно-аппаратных средств и их систем, разного рода сетей. Вредоносные программы можно подразделить на следующие виды.

1. Вирус (*Virus, Computer virus*) представляет собой самораспространяющийся вредоносный программный код, программу, активно размножающуюся путем создания и распространения своих копий, которые впоследствии могут быть модифицированы. Такая вредоносная программа скрытым образом проникает в память компьютера и занимает как оперативную память, так и дисковое пространство, поражает различные файлы в системе (например, документы), а также препятствует исправному функционированию программ, может содержать в себе разрушающие составные элементы, что способствует причинению значительного ущерба. Вирусы также подразделяются на загрузочные, файловые, почтовые вирусы.

2. Червь (*Worm*) является одной из форм компьютерного вируса, не осуществляющей изменение или заражение уже существующих файлов в системе, а формирующей свои собственные файлы, составляющие «тело червя». В свою очередь, черви подразделяют следующим образом:

– файловые черви (*File worm*) создают свои копии в каких-либо папках под различными именами, присваивающимися в произвольном порядке либо в соответствии определенным алгоритмом (например, P2P-червь). Принцип их функционирования основывается на том, что пользователь при обнаружении неизвестного ему исполняемого файла (*Executable file*)[1] в папке активирует его выполнение;

– архивные черви (*Archive worm*) используют уже существующий либо формирующийся архив для добавления в него своей копии, а также опираются

[1] Исполняемый файл (*executable file*) — это файл, содержащий программу, которая готова непосредственно для выполнения определенной операционной системой.

на то, что при проверке различными антивирусами опция проверки существующих архивов пользователя зачастую отключена в целях сокращения времени на проведение такого сканирования, именно это способствует эффективной адаптации и размножению вредоносной программы данного вида;

– сетевые черви (*Net-worm*) имеют в своем арсенале встроенные функции для непосредственного взаимодействия с сетью и обеспечивают свое самостоятельное распространение на связанные с сетью компьютеры;

– почтовые черви (*Email-worm*) осуществляет саморассылку по всем имеющимся в адресной книге либо текстовых документах адресам электронных почт, или же генерирующимся в случайном порядке, с использованием для этого специализированных почтовых программ и сервисов (SMTP-серверы) [5, с. 58].

2. Троянский конь (троянская программа либо «троянец») (*Trojan horse*) выступает в роли вредоносной программы, предназначенной для скрытого сбора и отправки конфиденциальных пользовательских данных, а также других ресурсов компьютера жертвы по заданным заранее злоумышленниками адресам. Зачастую такая программа создается изначально для ввода пользователя в заблуждение, т. е. использует маскировку под полезную для пользователя программу. В реальности она содержит в своей структуре деструктивные недокументированные функции, которые начинают свою деятельность только после проникновения в систему.

3. Макровирус (*Macro virus*) представляет собой макрос[2], который выполняется в автоматическом режиме и содержится в каком-либо файле документа, а также видоизменяет структуру основного используемого пользователем приложения, т. е. при формировании нового либо открытии уже существующего документа возможно присоединение к последнему макровируса, который может удалять или повреждать данные файлов, воспроизводить визуальные эффекты, изменять настройки приложений и др.

4. Шпион (*Spy*) или программа-агент является вредоносной программой для несанкционированного сбора данных (пользовательских паролей и логинов). Выделяют следующие ее виды: клавиатурный шпион (*KeyLogger*)[3]; спуфер (*Spoofer*)[4]; сниффер (*Sniffer*)[5]; программа удаленного администрирования (*Remote ac-*

---

[2] Макрос — это последовательность команд, предназначенная для автоматизации какой-либо операции (например, в Microsoft Word — макрос для преобразования адреса в формат адресной книги уже установленной формы).

[3] Собирает и сохраняет информацию о последовательностях нажатия всех клавиш с их возможной последующей отправкой злоумышленникам (пароли, данные о регистрации, аутентификации, входе в систему).

[4] Осуществляет несанкционированный доступ к различным пользовательским паролям и логинам с помощью подражания формы входа в систему или регистрации с последующим выводом ошибки ввода пароля.

[5] Следит и переотправляет злоумышленникам данные, передающиеся непосредственно по кагалу сети; также используется как программа поиска паролей.

cess tool, *Backdoor*)[6]; троянский прокси (*Proxy*)[7]; эксплоит (*Exploit*)[8]; клей (*Dropper, Binder*)[9]; кликер (*Clicker*)[10]; «Звонилка» (*Dialer*)[11]; сканер портов (*Port scanner*)[12]; загрузчик (*Downloader*)[13]; «Шутка» (*Hoax, Joke*)[14]; рекламная программа (*AdWare, SpyWare*)[15]; хиджакер (*Hijacker*)[16]; руткит (*Rootkit*)[17]; DoS/DDos/Nuke[18] [6, с. 238–241].

Все вышеперечисленные виды вредоносных программ обладают следующими признаками:

1) способностью к копированию, видоизменению, уничтожению либо непосредственному блокированию определенной компьютерной информации, а также к обезвреживанию различных средств защиты последней;

2) отсутствием оповещения пользователя компьютерной информации (данных) конкретного устройства о направленности своих действий;

3) отсутствием предоставления такому пользователю выбора согласия либо несогласия на осуществление ими своих задач и цели [7, с. 48].

Также вредоносными программами можно считать и «полезные» программы, которые используются уже в целях несанкционированного копирования, видоизменения, уничтожения либо блокировки компьютерных данных, нарушения функционирования в работе различных программно-аппаратных средств и их систем, разного рода сетей. Таким примером может служить ис-

---

[6] Предоставляет злоумышленникам возможность управлять контролируемым компьютером на расстоянии.

[7] Прокси-сервер, который скрытым образом устанавливается на пользовательский компьютер и приводит к нарушению функционирования сети и самого компьютера в целом.

[8] Эксплуатирует уязвимости приложений, отвечающих за управление сетевыми портами.

[9] Осуществляет слияние вредоносной программы с полезной, копирует данные в несанкционированном порядке.

[10] Предназначена для увеличения трафика в целом, раскрутки сайтов путем посещения страниц, показа рекламы и др.

[11] Осуществляет звонок с модема на международные номера телефонов с завышенными тарифами в автоматическом порядке.

[12] Выполняет поиск открытых уязвимых сетевых портов, установление характеристик как программной, так аппаратной среды с целью их дальнейшего использования для проникновения на компьютер жертвы вредоносных программ.

[13] Предназначена для загрузки вредоносных программ с заданных заранее источников.

[14] Использует инсценировку пугающих пользователя событий, при реагировании на которые последний причиняет ущерб своему программному и аппаратному обеспечению.

[15] Отображает специальные рекламные окна либо перенаправляет пользователя на рекламные сайты.

[16] Осуществляет изменение настроек системы (изменение обоев на рабочем столе и др.), зачастую непосредственно настроек браузера (смена домашней страницы, поисковой системы и др.).

[17] Перехватывает системные привилегии и функции операционной системы.

[18] Атакуют удаленные сетевые компьютеры и воспрепятствуют доступу к данным.

пользование программы Remote Admin[19], которая сама по себе не является вредоносной, однако возможна и ее установка без уведомления и получения на то согласия пользователя компьютерного устройства для дальнейшего сбора и отправки конфиденциальных данных последнего, что будет расцениваться как преступление, а сама программа будет считаться вредоносной.

В целом можно представить следующий алгоритм действий судебного эксперта при исследовании обнаруженных вредоносных программ при производстве СКТЭ, подразделяющийся на несколько стадий:

1) подготовительное исследование вредоносных программ, включающее в себя поиск и выбор антивирусного продукта, подготовку стендового компьютера (чаще всего применяются виртуальные машины[20], которые позволяют работать в любой гостевой операционной системе на выбор с заданными настройками параметрами) [8, с. 54];

2) непосредственное исследование вредоносных программ [9, с. 134–135].

При производстве СКТЭ следует иметь в виду, что непосредственно понятие «вредоносная программа» в своей структуре имеет правовые и технические составляющие, последние из которых и представляют собой объект экспертного исследования СКТЭ. Именно поэтому судебный эксперт в области СКТЭ уделяет особое внимание именно на определенным техническим свойствам и параметрам программы, методам ее установки в систему, их несанкционированному использованию в последней либо определенным техническим дефектам и проблемам в функционировании существующих в системе программных продуктов. Так, вопрос о потенциальном распространении вредоносных программ, а именно о существовании каких-либо следов такого движения через конкретные съемные носители (например, наличие ISO-образа, записанного программой NERO и др.) либо сети (например, по электронной почте и др.) является чисто техническим.

В процессе проведения СКТЭ различного вида компьютерные вирусы и последствия их воздействия являются объектами изучения, о чем говорилось ранее. В таком случае перед судебным экспертом ставятся вопросы о непосредственном наличии/отсутствии компьютерного вируса в системе устройства, при условии его существования рассматриваются также вопросы о его характеристиках и степени влияния на функционирование всей системы в целом, определяется тип, вид, непосредственное название и т. д. При этом объектами исследования СКТЭ могут быть не только вредоносные программы и компьютерные вирусы, но и антивирусные

[19] Remote Admin — программа для мониторинга/администрирования различных имеющихся на удаленном компьютерном устройстве ресурсов.

[20] Виртуальная машина (virtual machine) — вычислительная машина заданной конфигурации, моделируемая для пользователя как аппаратными, так и программными средствами конкретной реально существующей вычислительной машины; это такая программная среда, которая внутри одной программной и (либо) аппаратной системы эмулирует работу другой программной и (либо) аппаратной системы.

программы. Антивирусная программа (*antivirus program*) является такой обслуживающей программой, которая необходима для борьбы с различного рода вредоносным обеспечением и последствиями его проникновения в систему [2, с. 14]. Она сканирует все заданные пользователем области технического устройства в поиске вредоносных программ и осуществляет диагностику обнаруженных зараженных файлов, устанавливает тип вредоносной программы. На практике распространен тот факт, что судебный эксперт в области СКТЭ после произведенного исследования представленного на экспертизу объекта фиксирует в своем заключении отсутствие каких-либо вирусов и вредоносных программ на последнем. Такое заключение следует признать некорректным, поскольку антивирусная программа может пропустить новейшие версии вирусов. Именно ввиду такой тонкости в заключении эксперта необходимо указывать, с помощью какого именно антивирусного продукта не было обнаружено заражение файлов, дату обновления базы данных антивируса, а также прописать, что файлов, идентифицируемых настоящим антивирусным продуктом как вредоносных, в процессе проведения исследования обнаружено не было.

Более того, судебные эксперты часто допускают такую ошибку, как удаление обнаруженного с помощью антивирусного продукта вируса, на которое у них отсутствует разрешение лица, назначившего или запросившего данную судебную экспертизу. Согласно общепринятому правилу, эксперт обязуется вернуть предоставленное ему на исследование вещественное доказательство после изучения и дачи заключения в отношении последнего в целости и состоянии, соответствующем первоначальному, при этом указание на наличие вредоносной программы в системе обязательно [10, с. 56–57].

В последние десятилетия наблюдается значительный рост преступности в сфере компьютерных преступлений (компьютерных технологий), средством совершения которых служит вредоносное программное обеспечение, также называемое программным-информационным оружием и изучаемое в рамках СКТЭ [11, с. 182]. Особенность настоящего процесса, характерная как для профессиональной, так и для социально-бытовой сферы, заключается в применении существующих методов защиты информации (ограничения доступа к ней) в целях сокрытия совершения преступления, а также методов уничтожения такой информации, способов собирания и передачи выявленных действий и непосредственно работу конкретного пользователя в сети Интернет. Эти направления заслуживают особого внимания при повышении профессионального уровня всех участников судопроизводства, в первую очередь — лиц, обладающих специальными познаниями, т. е. экспертов и специалистов, следователей.

Литература

[1] Аверьянова Т.В., ред. Судебная экспертиза. М., Норма, 2006.

[2] Усов А.И., ред. Производство судебной компьютерно-технической экспертизы. Ч. III. Специализированный словарь компьютерной лексики для экспертов судебной компьютерно-технической экспертизы. М., РФЦСЭ при Минюсте РФ, 2009.

[3] Уголовный кодекс РФ от 13.06.1996 № 63-ФЗ (ред. от 29.07.2017). Собрание законодательства РФ, 17.06.1996, № 25, ст. 2954.
[4] ГОСТ Р 57429-2017. Судебная компьютерно-техническая экспертиза: термины и определения. Термины и определения. М., Стандартинформ, 2017.
[5] Еременко С.П., Сапелкин А.И., Хитов С.Б. Классификация вредоносных программ. *Вестник Санкт-Петербургского университета ГПС МЧС России*, 2016, № 3, с. 55–61.
[6] Усов А.И., ред. Производство судебной компьютерно-технической экспертизы. Ч. IV. Актуальные комплексные экспертные задачи. М., РФЦСЭ при Минюсте РФ, 2011.
[7] Вехов В.Б. Вредоносные компьютерные программы как предмет и средство совершения преступления. *Расследование преступлений: проблемы и пути их решения*, 2015, № 2(8), с. 43–46.
[8] Кривенок А.М. Применение виртуальных машин при решении вопроса об обнаружении следов действий троянской программы (или вируса) выполняющейся при ее активизации на компьютере. *Теория и практика судебной экспертизы*, 2013, № 3(31), с. 53–55.
[9] Карпухина Е.С., Сидорова А.К. Исследование вредоносных программ при производстве судебной компьютерно-технической экспертизы. *Теория и практика судебной экспертизы*, 2008, № 3(11), с. 127–136.
[10] Усов А.И., ред. Производство судебной компьютерно-технической экспертизы. Ч. I. Общая часть II. Диагностические и идентификационные исследования аппаратных средств. М., РФЦСЭ при Минюсте РФ, 2009.
[11] Баюш А.А. Понятие, сущность и значение судебной экспертизы в условиях современного делопроизводства. *Студенческая научная весна, посвященная 165-летию со дня рождения В.Г. Шухова. Сб. тез. док. всерос. студ. конф.* М., Изд-во МГТУ им. Н.Э. Баумана, 2018, с. 181–182.

Баюш Анна Анатольевна — студентка кафедры «Юриспруденция, интеллектуальная собственность и судебная экспертиза», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

Научный руководитель — Хайретдинов Дмитрий Александрович, старший преподаватель кафедры «Юриспруденция, интеллектуальная собственность и судебная экспертиза», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

METHODICAL BASES OF RESEARCH OF SUPPOSEDLY MALICIOUS SOFTWARE WITHIN THE FRAMEWORK OF FORENSIC COMPUTER TECHNICAL ENQUIRY

A.A. Bayush annabayush@mail.ru
SPIN-code: 3271-9054

Bauman Moscow State Technical University, Moscow, Russian Federation

Abstract

The main guidelines for the study of supposedly malicious software in the framework of forensic computer-technical enquiry (FCTE), designated by authorized bodies and officials, are considered. The method of expert research is determined, methodological bases (recommendations) of the research as a whole are given, a parallel is hold between the concepts of "virus" and "malware". The general classification of modern malicious programs is presented and their general analysis is performed. The algorithm for the production of FCTE is described in the study of malicious software as a whole and its properties separately as an object of study for this forensic enquiry.

Keywords

Forensic enquiry, forensic expert, expert evidence, special knowledge, forensic computer technical enquiry (FCTE), malicious software (malware), malware classification

Received 04.04.2019

References

[1] Aver'yanova T.V., ed. Sudebnaya ekspertiza [Forensic enquiry]. Moscow, Norma Publ., 2006 (in Russ.).

[2] Usov A.I., ed. Proizvodstvo sudebnoy komp'yuterno-tekhnicheskoy ekspertizy. Ch. III. Spetsializirovannyy slovar' komp'yuternoy leksiki dlya ekspertov sudebnoy komp'yuterno-tekhnicheskoy ekspertizy [Proceeding of computer forensic examination. P. III. Specialized of computer vocabulary for experts of computer forensic examination]. Moscow, RFTsSE pri Minyuste RF Publ., 2009 (in Russ.).

[3] Ugolovnyy kodeks RF ot 13.06.1996 № 63-FZ (red. ot 29.07.2017) [the Criminal Code of the Russian Federation of 13.06.1996 no. 63-FZ (ed. of 29.07.2017)]. Sobranie zakonodatel'stva RF [Official gazette], 17.06.1996, no. 25, art. 2954 (in Russ.).

[4] GOST R 57429-2017. Sudebnaya komp'yuterno-tekhnicheskaya ekspertiza: terminy i opredeleniya. Terminy i opredeleniya [State Standard R 57429-2017. Forensic Information technology examination. Terms and definitions]. Moscow, Standartinform Publ., 2017 (in Russ.).

[5] Eremenko S.P., Sapelkin A.I., Khitov S.B. Classification of malware. *Vestnik Vestnik Sankt-Peterburgskogo universiteta GPS MChS Rossii*, 2016, no. 3, pp. 55–61 (in Russ.).

[6] Usov A.I., ed. Proizvodstvo sudebnoy komp'yuterno-tekhnicheskoy ekspertizy. Ch. IV. Aktual'nye kompleksnye ekspertnye zadachi [Proceeding of computer forensic examination. P. IV. Current complex expert problems]. Moscow, RFTsSE pri Minyuste RF, 2011 (in Russ.).

[7] Vekhov V.B. Malware as a subject and tool of crime commission. *Rassledovanie prestupleniy: problemy i puti ikh resheniya*, 2015, no. 2(8), pp. 43–46 (in Russ.).

[8] Krivenok A.M. Using virtual machines for solving problem of detecting Trojan (or virus) traces at its execution at the PC. *Teoriya i praktika sudebnoy ekspertizy*, 2013, no. 3(31), pp. 53–55 (in Russ.).
[9] Karpukhina E.S., Sidorova A.K. research on malware at proceeding computer forensic examination. *Teoriya i praktika sudebnoy ekspertizy*, 2008, no. 3(11), pp. 127–136 (in Russ.).
[10] Usov A.I., red. Proizvodstvo sudebnoy komp'yuterno-tekhnicheskoy ekspertizy. Ch. I. Obshchaya chast' II. Diagnosticheskie i identifikatsionnye issledovaniya apparatnykh sredstv [Proceeding of computer forensic examination. P. I. Main part II. Diagnostic and identity hardware study]. Moscow, RFTsSE pri Minyuste RF Publ., 2009 (in Russ.).
[11] Bayush A.A. [Conception, contents and meaning of forensic enquiry in conditions of nowdays clerical work]. *Studencheskaya nauchnaya vesna, posvyashchennaya 165-letiyu so dnya rozhdeniya V.G. Shukhova. Sb. tez. dok. vseros. stud. konf.* [Students science spring dedicated to 165 anniversary of Shukhov V.G. Coll. Abs. Russ. Stud. Conf.]. Moscow, Bauman MSTU Publ., 2018, pp. 181–182 (in Russ.).

Bayush A.A. — Student, Department of Law, Intellectual Property and Forensic Examination, Bauman Moscow State Technical University, Moscow, Russian Federation.

Scientific advisor — Khayretdinov D.A., Assist. Professor, Department of Law, Intellectual Property and Forensic Examination, Bauman Moscow State Technical University, Moscow, Russian Federation.