https://doi.org/10.30764/1819-2785-2018-13-3-109-115

Применение технологий JTAG и Chip-Off в исследовании мобильных устройств

А.Н. Яковлев[1,2], А.С. Данилова[2]

[1] Управление организации экспертно-криминалистической деятельности Главного управления криминалистики Следственного комитета Российской Федерации, Москва 105005, Россия

[2] ФГБОУ ВО «Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет)», Москва 105005, Россия

Аннотация. Статья посвящена вопросу извлечения данных с поврежденных мобильных устройств с помощью технологий JTAG и Chip-Off. Описаны практические эксперименты по извлечению данных с помощью интерфейса JTAG из телефона HTC модели Wildfire S и методом Chip-Off из телефона BQ модели S-4525 Vienna. Выявлены знания и навыки, необходимые эксперту в работе при использовании этих технологий.

Ключевые слова: *JTAG, Chip-Off, судебная компьютерно-техническая экспертиза, извлечение данных, восстановление данных*

Для цитирования: Яковлев А.Н., Данилова А.С. Применение технологий JTAG и Chip-Off в исследовании мобильных устройств // Теория и практика судебной экспертизы. 2018. Том 13. № 3. С. 109–115. https://doi.org/10.30764/1819-2785-2018-13-3-109-115

JTAG and Chip-Off Technologies in Computer Forensics

Aleksei N. Yakovlev[1,2], Anna S. Danilova[2]

[1] Department of Organization of Expert Activities of the General Directorate of Criminalistics (Criminalistics Center) of the Investigative Committee of the Russian Federation, Moscow 105005, Russia

[2] Bauman Moscow State Technical University (National Research University of Technology), Moscow 105005, Russia

Abstract. The article focuses on the issue of damaged handheld device data extraction with the help of JTAG and Chip-Off technologies. Practical experiments were conducted to extract data from an HTC Wildfire S phone using the JTAG interface and from a BQ S-4525 Vienna phone using the Chip-Off technology. Also discussed are the knowledge and skills required for successful application of these methods by practitioners.

Keywords: *JTAG, Chip-Off, computer forensics, extraction of data, data recovery*

For citation: Yakovlev A.N., Danilova A.S. JTAG and Chip-Off Technologies in Computer Forensics. *Theory and Practice of Forensic Science*. 2018. Vol. 13. No. 3. P. 109–115. (In Russ.). https://doi.org/10.30764/1819-2785-2018-13-3-109-115

В области судебной компьютерно-технической экспертизы методы Chip-Off и JTAG вызывают неподдельный интерес и одновременно опасения, поскольку эти технологии не только позволяют получить доступ к данным с обходом некоторых способов защиты (например, защиты информации паролем), но и восстановить данные с поврежденного устройства путем использования частично деструктивной технологии, что требует аккуратности.

Угрюмов Е.П. [1] дает определение JTAG: Joint Test Action Group – объединенная группа по вопросам тестирования, по имени которой названы методы тестирования БИС/СБИС без физического доступа к каждому их выводу и программирования микросхем программируемой логики с помощью JTAG-интерфейса. Позднее это сокращение стало прочно ассоциироваться с разработанным этой группой специализированным аппаратным интерфейсом на базе стан-

дарта IEEE 1149.1 (официальное название Standard Test Access Port and Boundary-Scan Architecture[1]). Интерфейс предназначен для подключения сложных цифровых микросхем или устройств уровня печатной платы к стандартной аппаратуре тестирования и отладки.

На текущий момент JTAG – это промышленный стандарт, и практически все сложные цифровые микросхемы оснащаются этим интерфейсом для:

– выходного контроля микросхем при производстве;

– тестирования собранных печатных плат;

– прошивки микросхем с памятью;

– отладочных работ при проектировании аппаратуры и программного обеспечения.

Компьютерно-технический эксперт почти никогда не знает заранее, с какими проблемами ему придется столкнуться при производстве экспертизы. Поскольку наиболее распространенными инструментами для извлечения данных из мобильных устройств являются программные продукты компаний Cellebrite и Oxygen Software, то используемые ими методы иногда не позволяют получить доступ к памяти мобильного устройства. В таких случаях наиболее приемлемыми инструментами являются технологии JTAG и Chip-Off [2].

Перечислим проблемы, с которыми может столкнуться эксперт при работе с JTAG:

1) в открытом доступе нет распиновки (обозначений и описания каждого контакта на микросхеме) точек JTAG на платах мобильных устройств;

2) не во всех телефонах есть JTAG интерфейс (устройства могут поддерживать другую технологию отладки, например UART);

3) на плате не указано, какие функциональные точки относятся именно к JTAG;

4) эксперт получает необработанные данные из микросхемы памяти, которые еще нужно декодировать и интерпретировать.

Работа JTAG-программатора основана на передаче сигналов по определенной комбинации функциональных линий связи. Расшифровка функциональных выводов:

– VCC – Positive supply voltage – питание,

– GND – Ground – заземление,

– TCK – Test Clock – тестовое тактирование,

– RTCK – Returned Test Clock output – выходной тактовый сигнал,

– TRST – Test Reset – инициализации порта тестирования,

– TDI – Test Data Input – вход тестовых данных,

– TMS – Test Mode Select – выбор режима тестирования,

– TDO – Test Data Output – выход тестовых данных,

– NRST – Reset – вывод сброса.

Для использования метода JTAG в целях извлечения данных эксперту необходимы программное и аппаратное обеспечение JTAG; проводное соединение, припой, флюс и паяльник; схема распиновки точек JTAG на плате мобильного устройства.

Chip-Off в судебной экспертизе – это технология, предполагающая извлечение микросхемы памяти из устройства, ее подготовку для снятия физического дампа памяти и последующее извлечение данных из этого дампа.

Трудности при использовании технологии Chip-Off:

1) существуют различные типы микросхем памяти, и для каждого типа нужен свой программатор;

2) при выпаивании микросхемы памяти ее уже нельзя вернуть на исходное место;

3) при перегревании платы во время выпаивания чипа памяти существует риск расслоения платы устройства, что влечет за собой полную его неработоспособность;

4) Chip-Off программатор стоит дорого, и не каждое экспертное подразделение может закупить программаторы для работы со всеми видами микросхем памяти.

Существует два вида NAND[2] памяти: TSOP и BGA. Основное отличие микросхем памяти типа TSOP – наличие контактов, расположенных вокруг внешнего края микро-

[1] JTAG. // Статья из Википедии – свободной энциклопедии. URL: https://ru.wikipedia.org/wiki/JTAG (дата обращения 10.12.2016).
So, What is this «JTAG Forensics» anyway? // Сайт компании Paraben. URL: https://www.paraben.com/blog/74-so-what-is-this-jtag-forensics-anyway (дата обращения 12.04.2017).
What is JTAG, Chip-off and ISP? // Сайт компании Teel Technologies. URL: http://www.teeltech.com/ufaqs/what-is-jtag-chip-off-and-isp/ (дата обращения 10.04.2017).

[2] NAND – архитектура построения флэш-памяти, которая предполагает выполнение записи данных методом квантового туннелирования электронов из области плавающего затвора транзистора в область истока. Запись данных в этом случае производится значительно быстрее, чем у флэш-памяти иной архитектуры; для уменьшения эффекта низкой скорости чтения, микросхемы NAND снабжаются внутренним кэшем [3, с. 256].

схемы, которые спаяны с платой. Демонтаж такого типа микросхем прост, хотя и требует максимальной аккуратности.

С микросхемами типа BGA[3] (Ball Grid Array – массив шариков) дела обстоят сложнее. Данные микросхемы имеют множество соединителей в виде шариков, припаянных к плате, и иногда микросхема памяти защищена эпоксидной смолой, что существенно затрудняет работу. Микросхемы BGA не имеют единого стандарта, и каждый производитель может разработать собственный тип микросхемы памяти, предполагающий в том числе иное расположение шаров.

Для работы с микросхемами TSOP необходимо иметь небольшое количество адаптеров для программаторов, так как конфигурация контактов в отличие от BGA почти универсальна. На фото 1 представлен один из распространенных Chip-Off программаторов.

Микросхемы BGA используют производители мобильных устройств, так как этот тип микросхем позволяет управлять большими объемами данных.

Chip-Off оборудование состоит из трех компонентов:

– аппаратных средств, считывающих память;

– адаптера, учитывающего топологию выводов подключаемой к нему микросхемы памяти;

– специализированного программного обеспечения на рабочей станции эксперта.

Для работы по такой технологии компьютерно-технический эксперт должен уметь определить выводы соединений JTAG; понимать топологию, схемотехнику, иные особенности современных мобильных устройств, знать об их модификациях; определять тип памяти исследуемого устройства; знать алгоритмы управления данными в нем. Кроме этого, нужно обладать навыками демонтажа и повторной сборки компонентов устройства. Важной составляющей успешного применения любого из двух методов является знание организации данных на микросхемах памяти.

Рассмотрим эксперименты по извлечению данных с помощью интерфейса JTAG из телефона HTC модели Wildfire S и метода Chip-Off из телефона BQ модели S-4525 Vienna.

Для паяльных работ подготовили флюс FluxPlus, припой-катушку ZD-162 ПОС60 0,5 мм 250 г с флюсом, обмотку для снятия излишка припоя, очиститель-спрей CRAMOLIN FLUX-OFF и паяльник. Также необходимы нижний инфракрасный подогрев, специальный фен и программатор JTAG RIFF Box.

Поиск в сети Интернет схемы распиновки JTAG для телефона HTC Wildfire S позволил найти видео на сайте YouTube с демонстрацией основных операций работы с устройством[4].

На первом шаге необходимо разобрать корпус мобильного устройства. Далее припаяем медные проводники к контрольным точкам JTAG. Для удобства каждый проводник маркируем наклейкой с указанием линии связи. На фото 2 показано соединение платы телефона с программатором RIFF JTAG Box с помощью проводников. Линия сигнала VCC не подключена к программато-

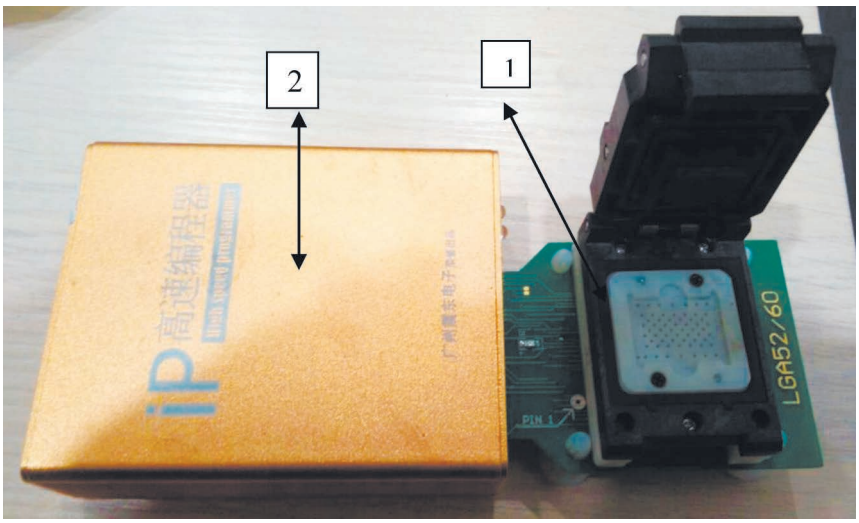

Фото 1. Chip-Off программатор; 1 – адаптер, 2 – считывающее аппаратное устройство

***Photo 1**. Chip-Off programmer; 1 – adapter, 2 – chip reader*

[3] Чипы, мосты, BGA микросхемы – что это? // Сайт сервисного центра «MultiOn». URL: http://laptop-sc.ru/bga.html (дата обращения: 20.04.2017).

[4] Riff Box JTAG – HTC Wildfire S – Boot Repair – Rom Install // Видео с демонстрацией метода JTAG для извлечения данных с мобильного устройства. URL: https://www.youtube.com (дата обращения 15.12.2016).

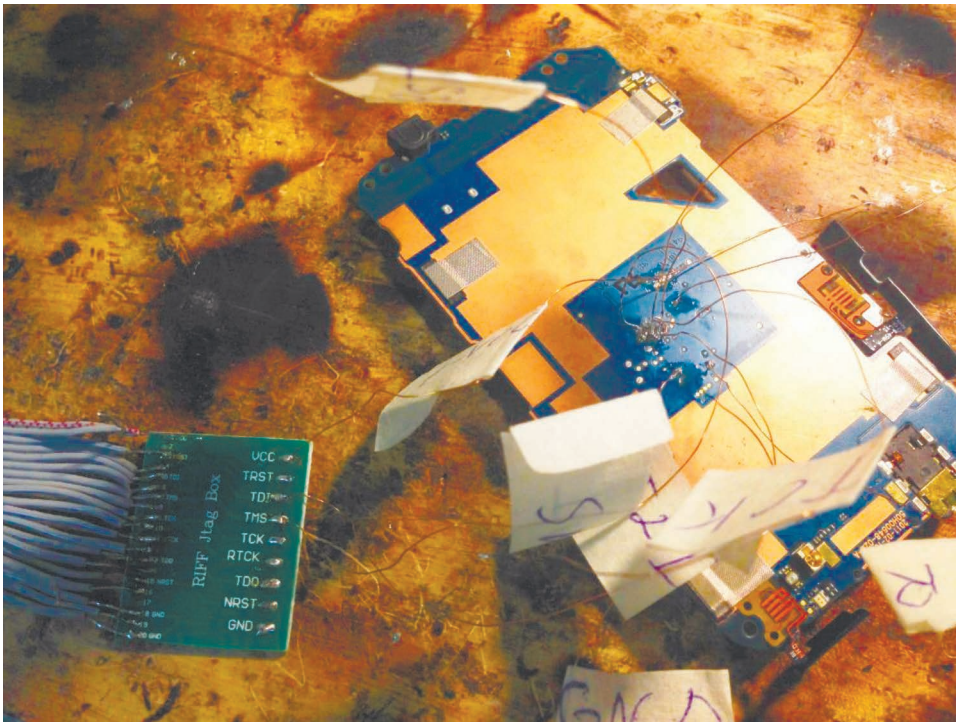

Фото 2. Вид платы мобильного телефона с соединением контрольных точек JTAG и разъемов RIFF JTAG Box

Photo 2. *A mobile phone PCB with JTAG Test Access Ports connected to a RIFF JTAG Box adapter*

ру, так как питание подается отдельно, когда уже происходит извлечение данных.

После соединения мобильного телефона и устройства RIFF JTAG Box программатор подключается к рабочей станции эксперта с установленной программой от производителя RIFF Box (можно скачать программу с официального сайта[5]). При первом подключении программатора требуется его регистрация. После прохождения этой процедуры устройство необходимо перевести в нужный режим, после чего программатор связывается с сервером для получения инструкций по работе с зарегистрированным устройством, что включает порядок подачи сигналов на плату и порядок получения дампа памяти мобильного устройства.

При использовании метода Chip-Off первоначальные действия будут аналогичны таковым при работе по технологии JTAG. Продемонстрируем это на конкретном примере.

В качестве объекта взят телефон и выполнена его разборка. В результате обнаружен защитный экран микросхемы, который впаян в плату, под ним видна микросхема памяти. Для снятия защитного экрана плата была разогрета феном, после нагрева защитный экран был извлечен (фото 3).

Под защитным экраном обнаружена микросхема памяти Kingston (фото 4). Для ее выпаивания применен инфракрасный нижний подогрев, который обеспечивает равномерность нагрева выводов микросхемы. Особенностью этой операции является предварительная обработка стыка корпуса микросхемы и платы флюсом, что создает безвоздушную среду между микросхемой и корпусом и ускоряет процесс нагрева (фото 5).

При нагреве платы необходимо обеспечить равномерный нагрев и контроль температуры. Для этого используется специализированная паяльная станция с контролем нагрева. При выпаивании нужного элемента монтажной схемы следует быть аккуратным во избежание повреждения находящихся рядом элементов.

После выпаивания микросхемы проводится операция реболлинга (удаления наплыва флюса и припоя с выводов микросхемы) при помощи очистителя-спрея CRAMOLIN FLUX-OFF (фото 6).

Извлеченную и подготовленную микросхему помещают в адаптер программатора, после чего из нее извлекаются данные, образующие после извлечения так называемый дамп памяти. Интерпретация

[5] RIFF Box // Сайт производителя программаторов RIFF Box. URL: http://www.riffbox.org (дата обращения 15.12.2016).

Фото 3. Подогрев платы феном со стороны впаянных выводов для снятия защитного экрана
Photo 3. *Heating the PCB with a blow dryer on the side with soldered pinouts to remove protective shielding*

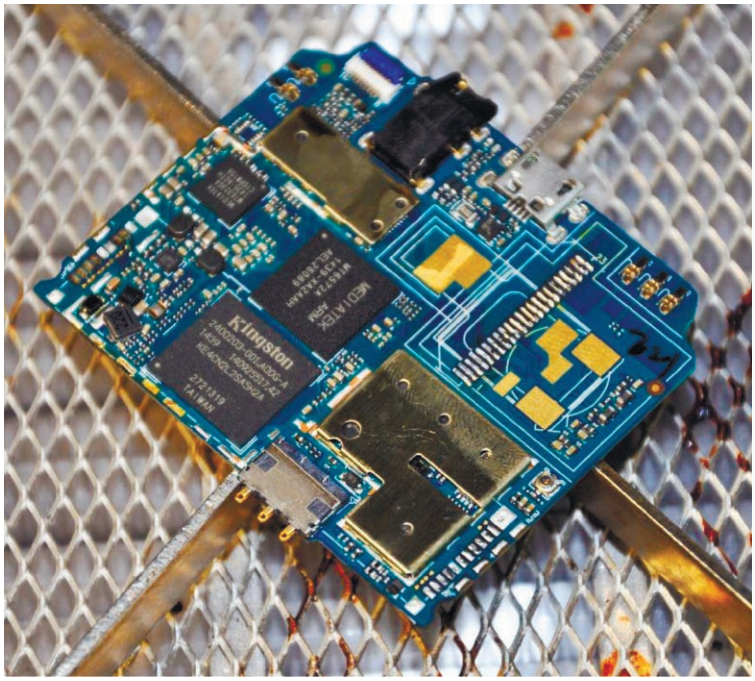

Фото 4. Плата телефона без защитного экрана
Photo 4. *Phone PCB without protective shielding*

их содержимого выполняется в штатном режиме при помощи специализированного программного обеспечения «Мобильный криминалист» (компании Oxygen Software) или комплексов UFED (компании Cellebrite).

Каждый из рассмотренных методов имеет свои плюсы и минусы. Метод Chip-Off выглядит деструктивным, но фактически таковым не является: объектом исследования в данном случае будет микросхема, целостность которой не вызывает сомнений. Кроме того, полученные результаты можно воспроизвести при повторной экспертизе.

Отметим, что для проведения исследования с применением технологий Chip-Off и JTAG необходимо получить разрешение следователя или лица, назначившего экспертизу, на конструктивную разборку мобильного устройства и выпаивание нужных для исследования микросхем памяти.

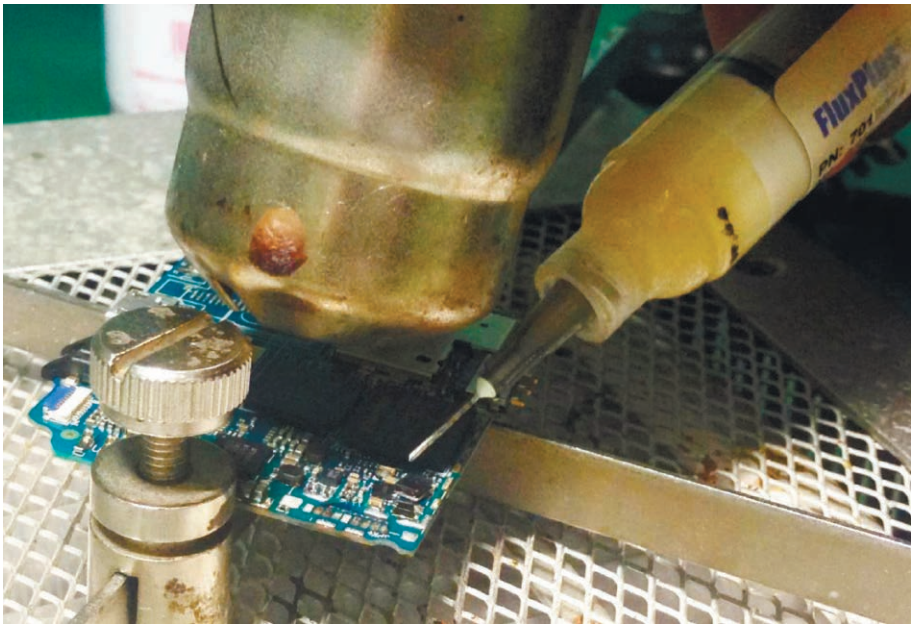

Фото 5. Нанесение флюса по контуру микросхемы памяти, нагрев верхней и нижней частей платы
Photo 5. *Applying flux along the memory chip contour while heating the top and bottom portions of the PCB*

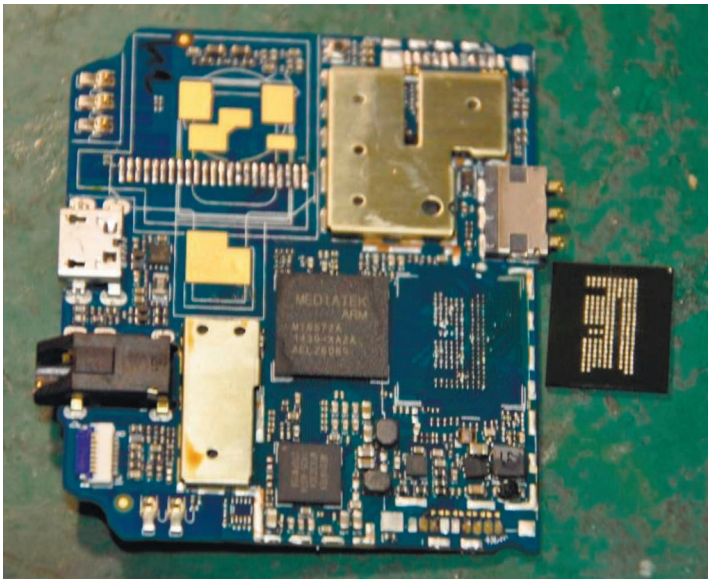

Фото 6. Выпаянная микросхема памяти (справа) после операции реболлинга и плата мобильного устройства (слева)
Photo 6. *Desoldered memory chip (right) after reballing and the mobile device PCB (left)*

СПИСОК ЛИТЕРАТУРЫ

1. Угрюмов Е.П. Цифровая схемотехника: учеб. пособие для вузов. 3-е изд., перераб. и доп. СПб.: БХВ-Петербург, 2010. 816 с.
2. Elder B. Chip-Off and JTAG Analysis. URL: http://www.evidencemagazine.com/index.php?option=com_content&task=view&id=922.
3. Воройский Ф.С. Информатика. Энциклопедический словарь-справочник: Введение в современные информационные и телекоммуникационные технологии в терминах и фактах. М.: Физматлит, 2006. 768 с.

REFERENCES

1. Ugryumov E.P. *Digital circuitry: a textbook for universities.* 3rd ed. Saint Petersburg: BHV-Petersburg, 2010. 816 p. (In Russ.)
2. Elder B. Chip-Off and JTAG Analysis. URL: http://www.evidencemagazine.com/index.php?option=com_content&task=view&id=922
3. Voroiskii F.S. *Computer science. Encyclopedic reference dictionary: introduction to modern information and telecommunications technologies in terms and facts.* Moscow: Fizmatlit, 2006. 768 p. (In Russ.)

ИНФОРМАЦИЯ ОБ АВТОРАХ

Яковлев Алексей Николаевич – к. ю. н., доцент, заместитель руководителя отдела компьютерно-технических и инженерно-технических исследований Управления организации экспертно-криминалистической деятельности Главного управления криминалистики (Криминалистического центра) Следственного комитета Российской Федерации, доцент кафедры юриспруденции, интеллектуальной собственности и судебной экспертизы Московского государственного технического университета им. Н.Э. Баумана (национальный исследовательский университет); e-mail: all-eks@mail.ru.

Данилова Анна Сергеевна – студент кафедры юриспруденции, интеллектуальной собственности и судебной экспертизы Московского государственного технического университета им. Н.Э. Баумана (национальный исследовательский университет); e-mail: annadanilova-bmstu@mail.ru.

ABOUT THE AUTHORS

Yakovlev Aleksei Nikolaevich – Candidate of Law, Associate Professor, Deputy Head of the Digital Forensics Division of the Department of Organization of Expert Activities of the General Directorate of Criminalistics (Criminalistics Center) of the Investigative Committee of the Russian Federation, Associate Professor of the Law, Intellectual Property and Forensics Department of the Bauman Moscow State Technical University (National Research University of Technology);e-mail: all-eks@mail.ru.

Danilova Anna Sergeevna – Student of the Law, Intellectual Property and Forensics Department of the Bauman Moscow State Technical University (National Research University of Technology); e-mail: annadanilova-bmstu@mail.ru.

Статья поступила 24.05.2018
Received 24.05.2018