УДК 343.983 DOI: 10.18698/2541-8009-2018-12-415

КРИМИНАЛИСТИЧЕСКОЕ ИССЛЕДОВАНИЕ СЛЕДОВ УСТАНОВКИ ПРЕДПОЛОЖИТЕЛЬНО КОНТРАФАКТНЫХ ПРОГРАММНЫХ ПРОДУКТОВ

А.В. Карлова carlova.anastasia@yandex.ru
SPIN-код: 8696-6670

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

Аннотация

Статья посвящена актуальным вопросам исследования предположительно контрафактных программных продуктов. На сегодняшний день контрафактная продукция в экономическом плане — это наиболее быстро развивающаяся часть теневого рынка. Пиратская продукция может быть обнаружена почти в любом государстве и в любом секторе экономики. Актуальность данной темы обусловлена тем, что рынок пиратской продукции в цифровом формате стабильно растет. Использование цифровых подделок будет только возрастать в связи с техническим прогрессом и быстрому распространению доступа к сети Интернет. Множество «пиратских» сайтов предлагают пользователю огромный выбор программ. Потребителям это не доставляет неудобств, а производители несут колоссальные денежные потери. Наибольшую популярность у нарушителей смежного и авторского права представляют аудио- и видеопродукция, компьютерные игры, операционные системы и программное обеспечение. В данной статье подробно рассмотрен такой объект преступного посягательства, как программное обеспечение.

Ключевые слова

Контрафактная продукция, авторские права, программное обеспечение, Defacto, классификация программного обеспечения, способы защиты программного обеспечения, киберпреступность, несанкционированное использование программных продуктов

Поступила в редакцию 09.11.2018

Введение. Борьба с контрафактной продукцией — одна из наиболее важных проблем современного мира. Распространение нелегальной продукции в России связано с социальными причинами. Большинство людей покупает нелегальные копии, потому что они намного дешевле лицензионной продукции, что более привлекательно для обычного человека. Анализ материалов следственной и судебной практики показывает, что за последние 10 лет среди преступлений, которые отличаются высокой степенью общественной опасности, не только нанося значительный материальный ущерб и моральный вред физическим и юридическим лицам, но и подрывая авторитет Российской Федерации на международной арене в сфере соблюдения конституционных прав и свобод человека и гражданина, возросло количество случаев нарушения авторских и

смежных прав, совершенных с использованием компьютерных и телекоммуникационных технологий [1, с. 141–142].

Компьютерные программы (программное обеспечение (ПО), или программы для ЭВМ) представляют собой один из объектов интеллектуальной собственности.

Законодательство РФ относит ПО к объектам авторского права (ст. 1259 Гражданского кодекса РФ [2]). Наиболее подвержены риску смежные и авторские права, которые регулируют отношения в области создания и использования произведений литературы, искусства и науки [3, с. 19].

Контрафактная продукция — это товар, производители которого нарушают интеллектуальные права владельцев путем использования идентичных качеств и характеристик, которые принадлежат оригинальному продукту, для введения в заблуждения потребителей и в целях недобросовестной конкуренции.

Преступники проявляют особый интерес к такому специфическому объекту авторского права, как программы для ЭВМ. Производитель программного продукта для извлечения максимальной прибыли обеспечивает как можно большее число пользователей продукта. Этим пользуются производители контрафактной продукции, когда устанавливают цены на пиратские копии ПО в несколько раз ниже по сравнению с лицензионными версиями.

На территории РФ киберпреступность, к которой в определенной степени можно отнести и производство контрафактных программных продуктов, имеет тенденцию к устойчивому росту.

Программное обеспечение — совокупность программных средств, которые реализуют функции накопления, обработки, анализа и хранения информации, а также предоставления к ней доступа пользователям информационной системы. С позиций предназначения и распространения ПО можно подразделить на три больших класса:

1) универсальное (отсутствие привязки к конкретной предметной области): системы обработки текстов, средства распознавания образов, системы управления базами данных, офисные системы, операционные системы, сетевое ПО, развлекательные компьютерные игры и т. п.;

2) специализированное (рассчитано на определенную группу пользователей, которые связаны с определенной предметной областью): системы автоматизированного проектирования, бухгалтерские, банковские и корпоративные системы, справочные и информационно-поисковые системы;

3) уникальное (разрабатывается по индивидуальному заказу для решения конкретной задачи и предназначено для использования организацией или лицом, которое сделало заказ [4, с. 163]).

Наибольший интерес для «пиратов» представляет универсальное и специализированное ПО, потому что оно предназначено для массового тиражирования.

Особенности установки и распространения ПО, работающего в среде операционной системы Windows. Для максимального удобства установки экземпляра программного продукта на жесткий диск некоторого компьютера

первоначально подготавливают установочный (дистрибутивный) экземпляр этого программного продукта.

Для автоматизации перечисленных действий разработчики ПО применяют особый программный продукт — инсталлятор. Получив инсталлятор, разработчик ПО оказывается обладателем дистрибутива программы, представляющего собой исполнимый файл и некоторые иные файлы, которые необходимо запустить на компьютере, где планируется установить программный продукт.

Традиционно встречаются имена файлов setup.exe, install.exe, но возможны и файлы с расширениями .diz, .nfo (в основном это пиратские и взломанные). Указанные файлы включаются во взломанный дистрибутив хакерскими группами, осуществляющими взлом коммерческих программных продуктов. В файлах содержится следующая информация [5, с. 23]:

– точные данные о названии взламываемой программы и ее версии;

– точные данные об исходном предназначении взламываемой программы;

– указание на порядок запуска взламываемой программы или на порядок ее взлома с помощью прилагаемых (разработанных хакерской группой) программных средств;

– краткие сведения о хакерской группе (ники, псевдонимы, реклама).

Данная информация ценна при производстве экспертизы предположительно контрафактных программных продуктов, поскольку хакерские группы проводят всесторонние глубокое исследование программы перед взломом и указывают наиболее точные сведения о программе.

После перепроверки экспертом часть таких сведений целесообразно включить в исследовательскую часть экспертного заключения или использовать при формулировании выводов.

По критерию оплаты и ее способам программы подразделяют на следующие категории [5, с. 24].

1. Бесплатные программы (Freeware). Бесплатные программы, распространяемые на условиях сохранения авторства разработчика; некоммерческого распространения любым лицом; запрета декомпилирования исполнимого файла.

2. Условно бесплатные (Shareware). Программы, предоставленные на некоторый срок или для некоторого количества запусков. Имеют функциональные ограничения. По наступлению оговоренного условия их необходимо удалить или оплатить их использование.

3. Демо-версии (Demo). Версии программ, специально созданные для демонстрации некоторых существенных особенностей программы, интерфейса. Предназначены для ознакомительных целей.

4. Adware. Программы, которые можно использовать бесплатно, но которые включают обязательный, ненужный пользователю, компонент (например, окно для трансляции рекламы).

5. Donationware. Программы, не имеющие функциональных ограничений, но оставляющие вопрос оплаты и ее размера на усмотрение пользователя.

Способы и средства защиты программных продуктов от неправомерной установки и использования. В век распространения контрафактной продукции разработчики программного продукта применяют определенные средства защиты, которые помогают защитить ПО от неправомерного доступа.

Первая группа способов защиты ПО от неправомерного использования основана на использовании уникальных регистрационных данных:

– s/n (serial number) — серийный номер, последовательность символов, которую можно ввести с клавиатуры; с использованием одного и того же серийного номера может быть активировано произвольное количество экземпляров программы, однако в некоторых случаях серийный номер создается персонально для каждого нового экземпляра;

– u/r — пара вида «имя пользователя / код активации», является функциональным аналогом серийного номера, однако зарегистрированный с его помощью экземпляр программы будет отображать сведения о том, что он зарегистрирован на пользователя с конкретным именем;

– cd-key — CD-ключ, аналог серийного номера, используется при распространении программных продуктов на компакт-дисках; в некоторых случаях каждый экземпляр программы при установке требует свой персональный CD-ключ;

– key — ключевой файл, последовательность символов, сохраненных в бинарном файле.

Вторая группа способов защиты ПО от неправомерного использования — создание и распространение trial-версий программ, обладающих ограниченным сроком использования.

Ограничение может касаться количества запусков или количества дней, прошедших с момента установки. Счетчик запусков или метка даты установки может храниться: в реестре, в ключевом файле, в специально отведенной области жесткого диска [6, с. 187]. Однако хакеры находят все более новые способы обхода защиты программного продукта. Наличие средств обхода защиты от несанкционированного использования является признаком контрафактного программного продукта.

Способы и средства неправомерной установки и использования программных продуктов. Для того чтобы обойти средства защиты, существуют определенные аппаратные, программные и информационные методы.

Общие признаки несанкционированного использования программы:

1) программа нуждается в дополнительной обработке: копировании дополнительных файлов и каталогов программы; замене одних файлов другими;

2) после установки программы требуется генерация серийных номеров или других ключевых данных. Имеются текстовые файлы (имена serial, serial.txt или иные), не входящие в состав легального дистрибутива и содержащие строку key или аналогичную с ключевыми данными;

3) после установки требуется запуск других исполнимых файлов, в том числе с именами crack, keygen, keymaker и т. п.;

4) наличие файлов .nfo, .diz, содержащих описание порядка преодоления средств технической защиты авторского права;

5) запуск программы осуществляется не с помощью файла, в имени которого отображается название программы, а файлом loader.exe;

6) перед запуском программы нужно обязательно запускать другую программу файлом с именем emulator.

Для неправомерной установки характерна установка программы на большее количество компьютеров, чем предусмотрено лицензионным соглашением. Этот способ используется в том случае, когда отсутствуют средства защиты от несанкционированного копирования программы;

Способы обхода средств защиты от несанкционированного копирования, предусмотренных правообладателем, подразделяют на программные, аппаратные (физические) и информационные.

Программные способы обхода средств защиты ПО:

1) Patch — программа для модификации исполнимых файлов ПО;

2) KeyGen — программа для генерации серийных номеров, используемых при регистрации ПО;

3) KeyMaker — программа для генерации ключевых файлов используемых при регистрации ПО;

4) Loader — программа, запускающая исполнимый файл ПО и модифицирующая загруженный в память код и/или данные ПО;

5) Emulator — программа-драйвер, эмулирующая работу аппаратных устройств (электронных ключей);

6) программы, вносящие изменения в реестр операционной системы.

Аппаратные (физические) способы обхода средств защиты ПО:

1) применение фальшивых электронных ключей; копий («клонов») электронных ключей;

2) копирование электронных носителей информации, выступающих в роли ключей (защищенных от копирования).

Информационные способы обхода средств защиты ПО:

1) распространение серийных номеров (использование одного серийного номера при регистрации нескольких экземпляров ПО);

2) распространение ключевых файлов — использование одного ключевого файла при регистрации нескольких экземпляров ПО;

3) распространение REG-файлов, содержащих информацию о серийном номере;

4) распространение образов дисков, содержащих дистрибутивы ПО;

5) распространение модифицированных файлов ПО;

6) использование ложных серверов регистрации/активации.

В рамках судебной экспертизы возможно исследование программного продукта на наличия данных средств обхода защиты от несанкционированного использования. Либо поиск таких средств на носителях информации.

По делам, связанным с нарушением прав интеллектуальной собственности, а именно изготовлением и распространением аудиовизуальной и музыкальной продукции, следователи нередко задают вопрос следующего содержания: «Является ли представленная продукция контрафактной?» Однако такой вопрос не может быть задан эксперту, так как понятие контрафакции является сугубо юридическим, а эксперт не вправе давать юридическую оценку исследуемого объекта, он может лишь выявить признаки соответствия или несоответствия объекта представленным образцам. Окончательный вывод о контрафактности продукции может сделать лишь компетентное лицо (следователь, суд) на основании подтверждения юридического факта разрешения правообладателя на изготовление или распространение объекта интеллектуальной собственности [7, с. 410].

При рассмотрении этого направления необходимо отдельно остановиться на определении технических признаков нелицензионного ПО на жесткий диск компьютера. К ним относятся:

1) несоответствие серийного номера (ProductID), зафиксированного в реестре операционной системы (при инсталляции программного продукта его регистрационные данные фиксируются в реестре экземпляра операционной системы), и номера на лицензионной карточке;

2) совпадение серийных номеров (ProductID) программных продуктов, что означает их установку с одного информационного носителя (при установке экземпляров операционной системы Windows с использованием ProductKey (ключа) ProductID будет различаться в зависимости от даты и времени установки и типа исходного носителя для обычных версий — в последних пяти знаках, для OEM-версий (это версии продуктов, предназначенные для поставки вместе с аппаратным обеспечением, т. е. программное обеспечение, которое поставляется вместе с компьютером в виде предустановленной версии) — в первых пяти знаках);

3) совпадение ключа продукта (ProductKey) программных продуктов, установленных на разных компьютерах;

4) установка OEM-версий на жестких дисках персональных компьютеров, приобретенных отдельно от ПО (они распространяются лицензированными продавцами компьютерной техники только при одновременной покупке новых компьютеров и ПО);

5) наличие программ-патчей, снимающих программную защиту лицензионного ПО;

6) наличие программ KeyGen, генерирующих ключи, необходимые для активации лицензионного ПО [8, с. 555].

Дальнейшее исследование сводится к решению проблемы определения инсталлированного ПО и его регистрационных данных. Эту задачу решают с помощью анализа системного реестра компьютера и каталога размещения инсталлированного ПО; осмотр дерева каталогов на предмет обнаружения дистрибутивов ПО и файлов программ, инсталляция которых не требуется.

Файлы устанавливаемого (инсталлируемого) ПО, как правило, размещаются в стандартном каталоге, определяемом операционной системой для этих це-

лей (для операционных систем Windows это каталог C:\Program Files и C:\Program Files (x86)). Анализ содержимого указанных каталогов и сравнение результатов с анализом системного реестра позволяет эксперту делать вывод о наличии инсталлированных экземпляров ПО.

Для получения аргументированных выводов экспертное исследование требует применение специальных познаний в различных областях науки и техники и должны обладать комплексным характером [9, с. 129].

Основными характеристиками пиратских программных продуктов могут быть:

1) неполный по своему содержанию и структуре программный пакет;

2) объединенные на одном носителе разнородные программные продукты Soft;

3) прилагающиеся к программам файлы с текстовым содержанием номера программного продукта Serial;

4) наличие специальной информации Readme о том, как обойти способ защиты программного продукта при установке на компьютер;

5) наличие встроенного регистрационного номера в устанавливаемых программах. Данное обстоятельство говорит о массовом использовании одного и того же подобранного номера разными пользователями, что в свою очередь, не дает им права обновлять установленную программу с официального сайта — разработчика ПО;

6) наличие файла ключа, например с расширением .key, дающего возможность беспрепятственно пользоваться программой в течение определённого времени;

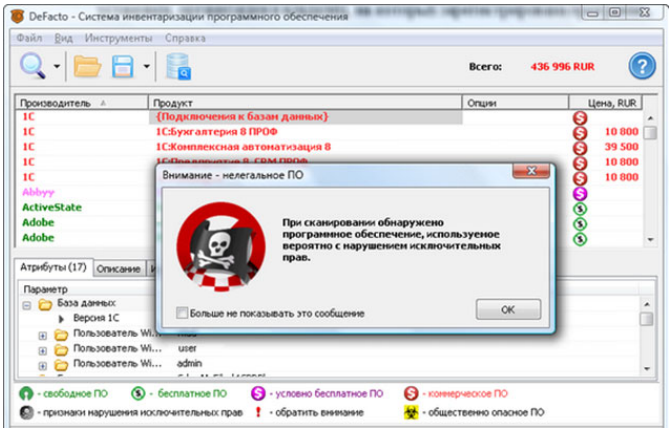
7) имеющиеся файлы типа KeyGen или Crack для создания в процессе генерации регистрационных электронных ключей (эмуляторов) или специального подавления требования программы о регистрации, иными словами, взломов парольной защиты лицензионного ПО [10, с. 565].

Однако на данный момент существуют и специальные программы, которые предназначены для выявления контрафактного ПО. Одна из них — Defacto.

Программа Defacto разработана ООО «ИнфоБиС» в сотрудничестве с ООО «Национальный центр по борьбе с преступлениями в сфере высоких технологий». Она позволяет существенно ускорить производство компьютерных экспертиз и исследований и упростить проведение проверок, направленных на выявление преступлений, связанных с нарушением исключительных прав.

Рассмотрим функции и возможности данного программного обеспечения. После запуска активированной программы, открывается основное окно программы [11].

После нажатия кнопки «Сканировать этот компьютер» начинается проверка (сканирование) активной системы, на которой запущена программа, с целью определения установленного ПО. После окончания проверки на экран выводится список обнаруженного ПО.



Окно с результатами сканирования в программе Defacto

В том случае, если на компьютере обнаружено ПО с признаками нарушения исключительных прав, выдается всплывающее окно с соответствующим предупреждением (см. рисунок). Видно, что на исследуемом компьютере обнаружен предположительно контрафактный коммерческий программный продукт «1С».

Список обнаруженного ПО представлен в виде таблицы, состоящей из полей «Производитель» (разработчик ПО), «Продукт» (название ПО), «Опции» (например, язык программы, если это влияет на ее стоимость), «Цена».

Если в поле «Производитель» перед названием разработчика ПО стоит «черная метка», это значит, что обнаружен признак нарушения исключительных прав (например, серийный номер данного ПО скомпрометирован и известен как рекомендуемый для неправомерной активации).

Различные программные продукты выделяются разным цветом:

– красный (коммерческие программы, для которых не существует бесплатных версий);

– фиолетовый (коммерческие программы, для которых существуют бесплатные версии demo, trial, shareware);

– зеленый (бесплатные программы, например, распространяющиеся с открытым кодом);

– черный (программы, сведения о которых отсутствуют в базе знаний).

В ходе своей работы и анализа зарегистрированной на исследуемом компьютере информации программа Defacto выявляет и сообщает пользователю о выявленных ей признаках нарушения исключительного права на ПО. К числу таких признаков относятся:

1) скомпрометированные регистрационные ключи, коды и серийные номера, которые рекомендуются для неправомерной активации (регистрации) программ нелицензионным пользователям;

2) наличие установленных и используемых на компьютере ПО для обхода технических средств защиты авторских прав — эмуляторов электронных ключей;

3) несоответствие между версией ПО и регистрационными ключами, между кодом продукта и серийным номером, и т. п.

Применение специального ПО Defacto позволяет существенно ускорить производство компьютерных экспертиз для выявления контрафактного программного продукта. Данное ПО повысило скорость и качество проведения экспертиз.

Результаты, которые выдает программа, максимально приближены к той форме, которая удобна для копирования с целью размещения в заключении эксперта или справке специалиста. Однако любая программа — лишь инструмент в руках профессионала. Каждый эксперт или специалист должен понимать, что в случае возникновения сомнений он может перепроверить полученные результаты с помощью других программных средств или вручную, поскольку дает заключение и несет за него ответственность именно человек, а не программа.

Заключение. Обобщая вышеизложенное, отметим, что в вопросах борьбы с контрафактной и фальсифицированной продукцией нет универсального решения проблемы. Об этом свидетельствует и опыт развитых стран: в Европейском Союзе, например, потребовалось около 40 лет, прежде чем были созданы условия, существенно ограждающие рынок ЕС от фальсифицированной продукции.

Анализ всего вышеизложенного позволяет сделать следующий вывод: понимание большой общественной опасности контрафактных действий и их широкая разнообразность говорить о том, что эффективная борьба с ними возможна при тесном сотрудничестве и взаимодействии органов, которые осуществляют обеспечение безопасности и качества товаров, работ, услуг.

Нарушителям авторского права и смежных прав невыгодно реализовывать товар с использованием чужого интеллектуального ресурса на обычных рынках, поэтому они используют иную, виртуальную площадку — Интернет. И это является серьезной проблемой уже нового уровня, ведь традиционные и опробованные методы борьбы с контрафактом здесь уже не срабатывают.

Таким образом, проблема борьбы с контрафактной продукцией в настоящее время является актуальной и требующей пристального внимания. Только в результате активного взаимодействия правообладателей, общественности и соответствующих уполномоченных госструктур можно воспрепятствовать получению прибыли теневыми структурами и пересечь незаконное использование объектов авторского и смежного права недобросовестными «предпринимателями».

Литература

[1] Вехов В.Б. *Основы криминалистического учения об исследовании и использовании компьютерной информации и средств ее обработки*. Волгоград, ВА МВД России, 2008, 408 с.

[2] Федеральный закон от 18 декабря 2006 г. № 230-ФЗ «Гражданский кодекс РФ. Часть четвертая» (ред. от 23.05.2018). Парламентская газета, № 214-215, 21.12.2006.

[3] Мэггс П.Б., Сергеев А.П. *Интеллектуальная собственность*. Москва, Юристъ, 2000, 400 с.

[4] Лабутин Н.Г. Контрафактность программного обеспечения и информационная безопасность. *Контрафактность как угроза экономической безопасности России*. Нижний Новгород, Нижегородская академия МВД России, 2006, с. 161–181.

[5] Яковлев А.Н., Юрин И.Ю., Шухнин М.Н., Яровой С.П. *Контрафактное программное обеспечение: профессиональный подход*. Саратов, Научная книга, 2007, 80 с.

[6] Нехорошев А.Б., Шухнин М.Н, Юрин И.Ю., Яковлев А.Н. *Практические основы компьютерно-технической экспертизы*. Саратов, Научная книга, 2007, 266 с.

[7] Идрисова С.Ф. Криминологические аспекты преступлений, связанных с реализацией контрафактной продукции. *Контрафактность как угроза экономической безопасности России*. Нижний Новгород, Нижегородская академия МВД России, 2006, с. 407–415.

[8] Костин П.В., Крыгин С.В. Особенности исследования машинных носителей информации при расследовании преступлений, возбужденных по ст. 146 УК РФ. *Контрафактность как угроза экономической безопасности России*. Нижний Новгород, Нижегородская академия МВД России, 2006, с. 550–561.

[9] Аристова Н.Л. Контрафактная продукция: основные признаки. *Контрафактность как угроза экономической безопасности России*. Нижний Новгород, Нижегородская академия МВД России, 2006, с. 126–130.

[10] Лапшин В.Е. Место специальных познаний в раскрытии и расследовании преступлений о контрафактной продукции. *Контрафактность как угроза экономической безопасности России*. Нижний Новгород, Нижегородская академия МВД России, 2006, с. 561–567.

[11] Defacto. URL: http://www.defacto-com.ru/ (дата обращения 13.09.2018).

Карлова Анастасия Владимировна — студентка кафедры «Юриспруденция, интеллектуальная собственность и судебная экспертиза», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

FORENSIC INVESTIGATION OF THE INSTALLATION OF ALLEGEDLY COUNTERFEIT SOFTWARE PRODUCTS

A.V. Carlova
carlova.anastasia@yandex.ru
SPIN-code: 8696-6670

Bauman Moscow State Technical University, Moscow, Russian Federation

Abstract

The article is devoted to current research issues of allegedly counterfeit software products. Nowadays counterfeit products in economic terms are the fastest growing part of the shadow market. Pirated products can be found in almost any state and in any sector of the economy. The relevance of this topic is due to the fact that the market for pirated products in digital format is growing steadily. The use of digital fakes will only increase due to technical progress and to the rapid spread of access to the Internet. Many "pirated" sites offer the user a huge selection of programs. It does not cause inconvenience to consumers, but manufacturers incur enormous monetary losses. The most popular among violators of related and copyright are audio and video products, computer games, operating systems and software. This article describes in detail such an object of criminal encroachment as software.

Keywords

Counterfeit products, copyrights, software, Defacto, software classification, software protection methods, cybercrime, unauthorized using of software products

Received 09.11.2018

References

[1] Vekhov V.B. Osnovy kriminalisticheskogo ucheniya ob issledovanii i ispol'zovanii komp'yuternoy informatsii i sredstv ee obrabotki [Fundamentals of forensic theory on research and usage of computer information and its processing technique]. Volgograd, VA MVD Rossii publ., 2008, 408 p.

[2] Federal'nyy zakon ot 18 dekabrya 2006 g. № 230-FZ "Grazhdanskiy kodeks RF. Chast' chetvertaya" (red. ot 23.05.2018) [Federal law of 18.02.2006 no. 230-FZ "Civil Code of the RF" (ed. of. 23.05.2018)]. *Parlamentskaya gazeta*, no. 214-215, 21.12.2006.

[3] Meggs P.B., Sergeev A.P. Intellektual'naya sobstvennost' [Intellectual property]. Moscow, Yurist publ., 2000, 400 p.

[4] Labutin N.G. Kontrafaktnost' programmnogo obespecheniya i informatsionnaya bezopasnost' [Software counterfeit and informational security]. *Kontrafaktnost' kak ugroza ekonomicheskoy bezopasnosti Rossii* [Counterfeit as a threat to economic safety of Russia]. Nizhniy Novgorod, Nizhegorodskaya akademiya MVD Rossii publ., 2006, pp. 161–181.

[5] Yakovlev A.N., Yurin I.Yu., Shukhnin M.N., Yarovoy S.P. Kontrafaktnoe programmnoe obespechenie: professional'nyy podkhod [Counterfeit software: professional approach]. Saratov, Nauchnaya kniga publ., 2007, 80 p.

[6] Nekhoroshev A.B., Shukhnin M.N, Yurin I.Yu., Yakovlev A.N. Prakticheskie osnovy komp'yuterno-tekhnicheskoy ekspertizy [Practical fundamentals of computer-technical expertise]. Saratov, Nauchnaya kniga publ., 2007, 266 p.

[7] Idrisova S.F. Kriminologicheskie aspekty prestupleniy, svyazannykh s realizatsiey kontrafaktnoy produktsii [Criminological aspects of crimes, connected with realization of counterfeit production]. *Kontrafaktnost' kak ugroza ekonomicheskoy bezopasnosti Rossii* [Counterfeit as a threat to economic safety of Russia]. Nizhniy Novgorod, Nizhegorodskaya akademiya MVD Rossii publ., 2006, pp. 407–415.
[8] Kostin P.V., Krygin S.V. Osobennosti issledovaniya mashinnykh nositeley informatsii pri rassledovanii prestupleniy, vozbuzhdennykh po st. 146 UK RF [Special aspects of study on technical information carriers at the investigation of crimes based on 146 article of the Criminal Code of the RF]. *Kontrafaktnost' kak ugroza ekonomicheskoy bezopasnosti Rossii* [Counterfeit as a threat to economic safety of Russia]. Nizhniy Novgorod, Nizhegorodskaya akademiya MVD Rossii publ., 2006, pp. 550–561.
[9] Aristova N.L. Kontrafaktnaya produktsiya: osnovnye priznaki [Counterfeit production: main features]. *Kontrafaktnost' kak ugroza ekonomicheskoy bezopasnosti Rossii* [Counterfeit as a threat to economic safety of Russia]. Nizhniy Novgorod, Nizhegorodskaya akademiya MVD Rossii publ., 2006, pp. 126–130.
[10] Lapshin V.E. Mesto spetsial'nykh poznaniy v raskrytii i rassledovanii prestupleniy o kontrafaktnoy produktsii [A place of expertise in solution and investigation of counterfeit production crimes]. *Kontrafaktnost' kak ugroza ekonomicheskoy bezopasnosti Rossii* [Counterfeit as a threat to economic safety of Russia]. Nizhniy Novgorod, Nizhegorodskaya akademiya MVD Rossii publ., 2006, pp. 561–567.
[11] Defacto. Available at: http://www.defacto-com.ru/ (accessed 13 September 2018).

A.V. Carlova — student, Department of Law, Intellectual Property and Forensic Examination, Bauman Moscow State Technical University, Moscow, Russian Federation.