Научная статья
УДК 340.6
DOI 10.33184/vest-law-bsu-2023.20.9

Коваленко Анна Сергеевна
МГТУ им. Н.Э. Баумана,
Москва, Россия, kovalenko.as@bmstu.ru

ИССЛЕДОВАНИЕ ОБСТОЯТЕЛЬСТВ КОМПЬЮТЕРНОГО МОНТАЖА ДОКУМЕНТОВ МЕТОДАМИ СУДЕБНОЙ КОМПЬЮТЕРНО-ТЕХНИЧЕСКОЙ ЭКСПЕРТИЗЫ

Аннотация. В статье рассмотрены группы цифровых следов, образующихся в результате фальсификации документов методом компьютерного монтажа. Предложены методические рекомендации по обнаружению и анализу следов каждой группы, рассмотрено программное обеспечение для работы с указанными следами. Приведены результаты экспериментального исследования, основанного на описанных рекомендациях, которое заключалось в выполнении компьютерного монтажа документа и последующем анализе образовавшихся цифровых следов.

Ключевые слова: цифровые следы, компьютерный монтаж, компьютерно-техническая экспертиза, подделка документов, реквизиты документов, реестр операционной системы

Для цитирования: Коваленко А.С. Исследование обстоятельств компьютерного монтажа документов методами судебной компьютерно-технической экспертизы / А.С. Коваленко. – DOI 10.33184/vest-law-bsu-2023.20.9 // Вестник Института права Башкирского государственного университета. – 2023. – № 4. – С. 68–77.

Original article

Kovalenko Anna Sergeevna
Bauman Moscow State Technical University,
Moscow, Russia, kovalenko.as@bmstu.ru

INVESTIGATION OF THE CIRCUMSTANCES OF COMPUTER MODIFIED OF THE DOCUMENTS BY METHODS OF THE DIGITAL FORENSICS

Abstract. The article considers groups of digital traces formed as a result of the preparation of documents by computer modified. Methodological recommendations for the detection and analysis of traces of each group are proposed, software for working with these traces is considered. The results of an experimental study based on the described recommendations, which consisted in performing computer modified of the document and subsequent analysis of the resulting digital traces, are presented.

Keywords: digital traces, computer modified, digital forensics, document forgery, details of documents, operating system registry

For citation: Kovalenko A.S. Investigation of the Circumstances of Computer Modified of the Documents by Methods of the Digital Forensics. *Vestnik Instituta prava Bashkirskogo gosudarstvennogo universiteta = Bulletin of the Institute of Law of the Bashkir State University,* 2023, no. 4, pp. C. 68–77. (In Russian). DOI 10.33184/vest-law-bsu-2023.20.9.

Целью назначения и производства судебной экспертизы является установление фактов и обстоятельств конкретного уголовного или гражданского дела, дела об административном правонарушении. Одной из задач при проведении экспертизы может выступать исследование следовой картины и восстановление последовательности действий при подделке документов методом компьютерного монтажа.

Современный уровень развития технологий в области обработки изображений позволяет осуществлять изготовление и обработку изображений таких реквизитов, как подписи, оттиски печатей и штампов, с помощью специализированного программного обеспечения (ПО), что, в свою очередь, может быть использовано в преступных целях для изготовления поддельных документов. В этой связи становится актуальным исследование обстоятельств компьютерного монтажа документов, выявление и анализ следов использования графических редакторов и другого ПО, анализ последовательности действий при подготовке документа.

При осуществлении компьютерного монтажа оригинал документа сканируется на машинный носитель компьютера. Затем в полученном изображении путем графической обработки монтируются необходимые реквизиты, либо реквизиты с данного документа монтируются на другой документ, после чего документ может быть распечатан на принтере [1].

Предлагается выделить следующие группы цифровых следов, образующихся при компьютерном монтаже документа и подлежащих анализу в ходе экспертного исследования:

1) следы подключения сканеров, принтеров, МФУ, внешних накопителей данных;

2) следы работы с графическими редакторами;

3) следы работы с изображениями;

4) следы подготовки текста в текстовом редакторе.

В ходе исследования был проведен эксперимент, заключавшийся в поиске и анализе следов компьютерного монтажа документа. В качестве примера в текстовом редакторе MS Word был подготовлен документ, содержащий следующие реквизиты:

1) текст;

2) подпись, полученную из отсканированного ранее документа и обработанную с использованием графического редактора Adobe Photoshop;

3) два оттиска печатей, один из которых был выполнен в Paint.net, второй – при помощи специализированной программы для изготовления оттисков «Быстропечати».

В завершении исследуемый документ был распечатан.

В ходе выявления и анализа следовой картины были последовательно рассмотрены следы каждой из обозначенных групп. При поиске и анализе следов первой группы в первую очередь интерес представляет системный реестр Windows, для анализа которого может быть использовано ПО MiTeC Windows registry recovery и Regshot.

В системном реестре содержится информация обо всех подключавшихся к компьютеру устройствах, среди которых периферийные устройства МФУ HP LaserJet Professional M1132 MFP и принтер Canon g1010 series, использовавшиеся для сканирования и последующей печати документа (см. рис. 1).

Следы работы с периферийными устройствами также содержатся в журнале обработки .inf-файлов, в которых сохраняются настройки подключаемого оборудования. Данный журнал содержится в файле setupapi.dev.log (регистрационный путь: C:\Windows\INF) и может быть просмотрен в текстовом редакторе «Блокнот». К числу хранящейся в файле setupapi.dev.log информации относится дата и время подключения периферийных устройств.

Например, МФУ HP LaserJet Professional M1132 MFP было подключено 18.08.2022 в 20.51 (см. рис. 2).

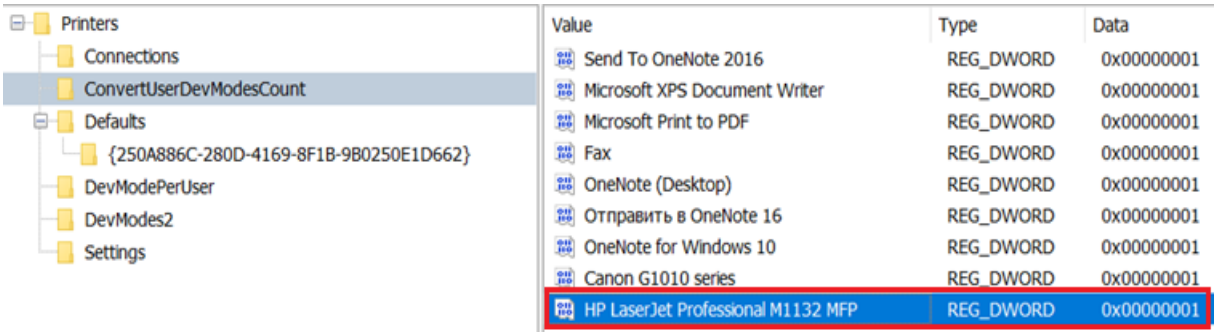


Рис. 1. Фрагмент окна программы MiTeC Windows registry recovery, сведения о подключавшихся устройствах

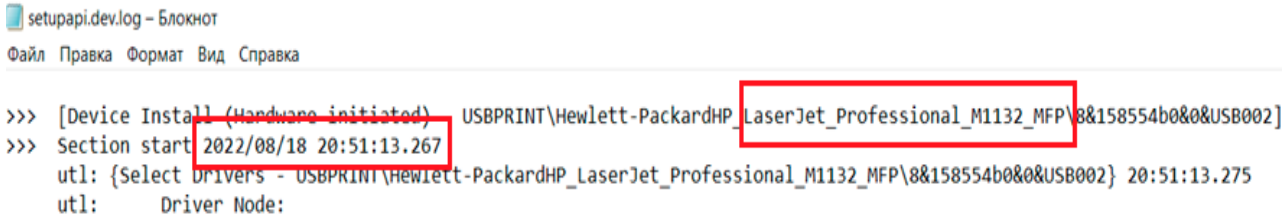


Рис. 2. Фрагмент окна программы «Блокнот», сведения о подключении МФУ HP LaserJet Professional M1132 MFP

Сведения об отправленных на печать документах могут быть получены путем изучения файлов очереди печати .SHD и .SPL с помощью программ SPL Viewer и SPLView. В ходе исследования файлов очереди печати было обнаружено изображение исследуемого документа (см. рис. 3).

Факт и время подключения внешних накопителей данных могут быть установлены при исследовании LNK-файлов – файлов ссылок на открываемые ресурсы [2, с. 219]. Регистрационный путь LNK-файлов:

– C:\%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent\

– C:\%USERPROFILE%\AppData\Roaming\Microsoft\Office\Recent\ (отдельно для файлов, открываемых программами пакета MS Office).

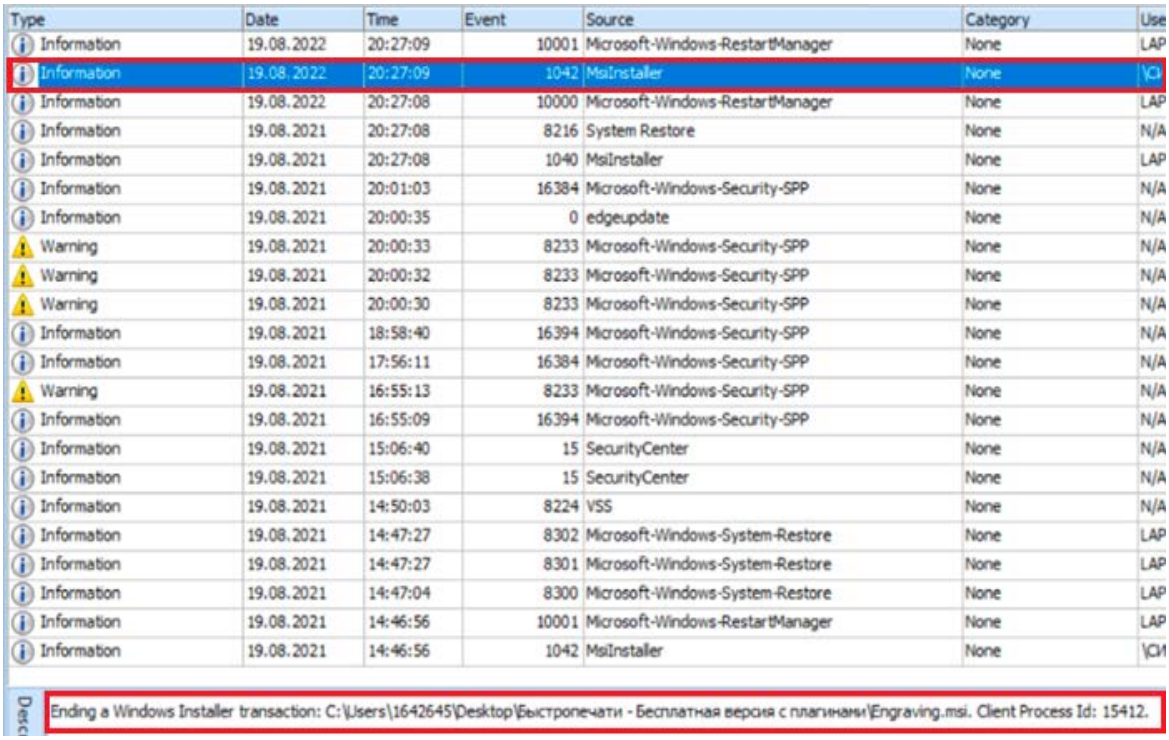
При выявлении подключавшихся к компьютеру внешних накопителей исследованию также подлежат журналы событий ОС, удаленные ранее файлы, файл подкачки [2, с. 102].

Для создания новых и обработки имеющихся в оригинале документа реквизитов используются графические редакторы. При подготовке реквизитов документа могут быть использованы как встроенные редакторы (Paint, Paint.net), так и специализированные (CorelDraw, Adobe Photoshop, Inkscape, Adobe Illustrator, Expression Design, GIMP и др.). Кроме того, существуют про-

граммы, позволяющие создавать отдельные реквизиты документов. Например, есть ряд программ, предназначенных для создания оттисков печатей и штампов: «Быстропечати», MasterStamp, «ШТАМП», «Печать Эксперт» (онлайн-сервис) и др.

Рис. 3. Фрагмент окна программы SPLView. Изображение документа, полученное при исследовании файлов очереди печати

Следы установки и запуска графических редакторов содержатся в системном реестре, журналах событий ОС, каталоге Prefetch. Каталог Prefetch сохраняет сведения о последних запущенных программах, среди которых Paint.net и Adobe Photoshop. В ходе анализа журналов событий могут быть получены сведения об инсталляции и (или) деинсталляции графических редакторов. В данном случае интерес в первую очередь представляет журнал программ AppEvent.Evt. Для просмотра системных журналов может быть использовано ПО Event Log Explorer и Log Viewer Plus. Например, в журнале AppEvent.Evt содержится информация об инсталляции (19.08.2022 в 20.27) и последующей деинсталляции (19.08.2022 в 21.03) программы «Быстропечати», предназначенной для создания оттисков печатей и штампов (см. рис. 4).



Type	Date	Time	Event	Source	Category	Use
Information	19.08.2022	20:27:09	10001	Microsoft-Windows-RestartManager	None	LAP
Information	19.08.2022	20:27:09	1042	MsiInstaller	None	\Cl
Information	19.08.2022	20:27:08	10000	Microsoft-Windows-RestartManager	None	LAP
Information	19.08.2021	20:27:08	8216	System Restore	None	N/A
Information	19.08.2021	20:27:08	1040	MsiInstaller	None	LAP
Information	19.08.2021	20:01:03	16384	Microsoft-Windows-Security-SPP	None	N/A
Information	19.08.2021	20:00:35	0	edgeupdate	None	N/A
Warning	19.08.2021	20:00:33	8233	Microsoft-Windows-Security-SPP	None	N/A
Warning	19.08.2021	20:00:32	8233	Microsoft-Windows-Security-SPP	None	N/A
Warning	19.08.2021	20:00:30	8233	Microsoft-Windows-Security-SPP	None	N/A
Information	19.08.2021	18:58:40	16394	Microsoft-Windows-Security-SPP	None	N/A
Information	19.08.2021	17:56:11	16384	Microsoft-Windows-Security-SPP	None	N/A
Warning	19.08.2021	16:55:13	8233	Microsoft-Windows-Security-SPP	None	N/A
Information	19.08.2021	16:55:09	16394	Microsoft-Windows-Security-SPP	None	N/A
Information	19.08.2021	15:06:40	15	SecurityCenter	None	N/A
Information	19.08.2021	15:06:38	15	SecurityCenter	None	N/A
Information	19.08.2021	14:50:03	8224	VSS	None	N/A
Information	19.08.2021	14:47:27	8302	Microsoft-Windows-System-Restore	None	LAP
Information	19.08.2021	14:47:27	8301	Microsoft-Windows-System-Restore	None	LAP
Information	19.08.2021	14:47:04	8300	Microsoft-Windows-System-Restore	None	LAP
Information	19.08.2021	14:46:56	10001	Microsoft-Windows-RestartManager	None	LAP
Information	19.08.2021	14:46:56	1042	MsiInstaller	None	\Cl

Ending a Windows Installer transaction: C:\Users\1642645\Desktop\Быстропечати - Бесплатная версия с плагинами\Engraving.msi. Client Process Id: 15412.

Рис. 4. Фрагмент окна программы Event Log Explorer. Сведения об установке программы «Быстропечати»

При исследовании следов работы с графическими изображениями важно понимать, что при удалении самих изображений остаются их миниатюры [3, с. 191], которые сохраняются по регистрационному пути: C:\%USERPROFILE%\AppData\Local\Microsoft\Windows\Explorer [3]. Для просмотра файлов миниатюр предлагается использовать специальное ПО Thumbcache Viewer. Наличие в кэше миниатюр thumbcache_256.db (метки даты и времени: 19.08.2022, 12.34) изображений реквизитов свидетельствует об их предварительной обработке на конкретном компьютере (см. рис. 5).

Рис. 5. Фрагмент окна программы Thumbcache Viewer. Миниатюра изображения оттиска печати, обнаруженная в ходе исследования содержимого файла thumbcache_256.db

Следующая группа следов – следы подготовки текста документа в текстовых редакторах. Анализ следов данной группы должен включать в себя поиск и исследование автосохраненных и ранее удаленных документов. Для восстановления удаленных документов предлагается использовать программы Recuva, R.studio, GetDataBack. Например, к числу удаленных файлов, представляющих интерес для исследования обстоятельств подготовки экспериментального документа, относятся файлы с расширением .docx, содержащие фрагменты экспериментального документа, файлы графических форматов, содержащие фрагменты изображений подписи и оттисков печатей, а также файлы с расширениями .psd (проекты Adobe Photoshop) и .pdn (проекты Paint.net).

По результатам выявления и анализа следов рассмотренных групп для дальнейшего синтеза полученных данных в общую следовую картину предлагается использовать технологию Timeline. Временная шкала может быть построена при помощи специализированных программ (например, Autopsy), а также путем анализа файла ActivitiesCache.db, расположенного по регистрационному пути: C:\%USERPROFILE%\AppData\Local\ConnectedDevicesPlatform\L.%USERPROFILE%\ и содержащего историю событий, происходивших на компьютере [4]. Содержимое данного файла представляет собой базу данных SQLite и может быть просмотрено программой DB Browser for SQLite.

На основе выявленных следов, а также анализа содержимого файла ActivitiesCache.db по технологии Timeline была построена временная шкала, отражающая последовательность подготовки документа (см. рис. 6).

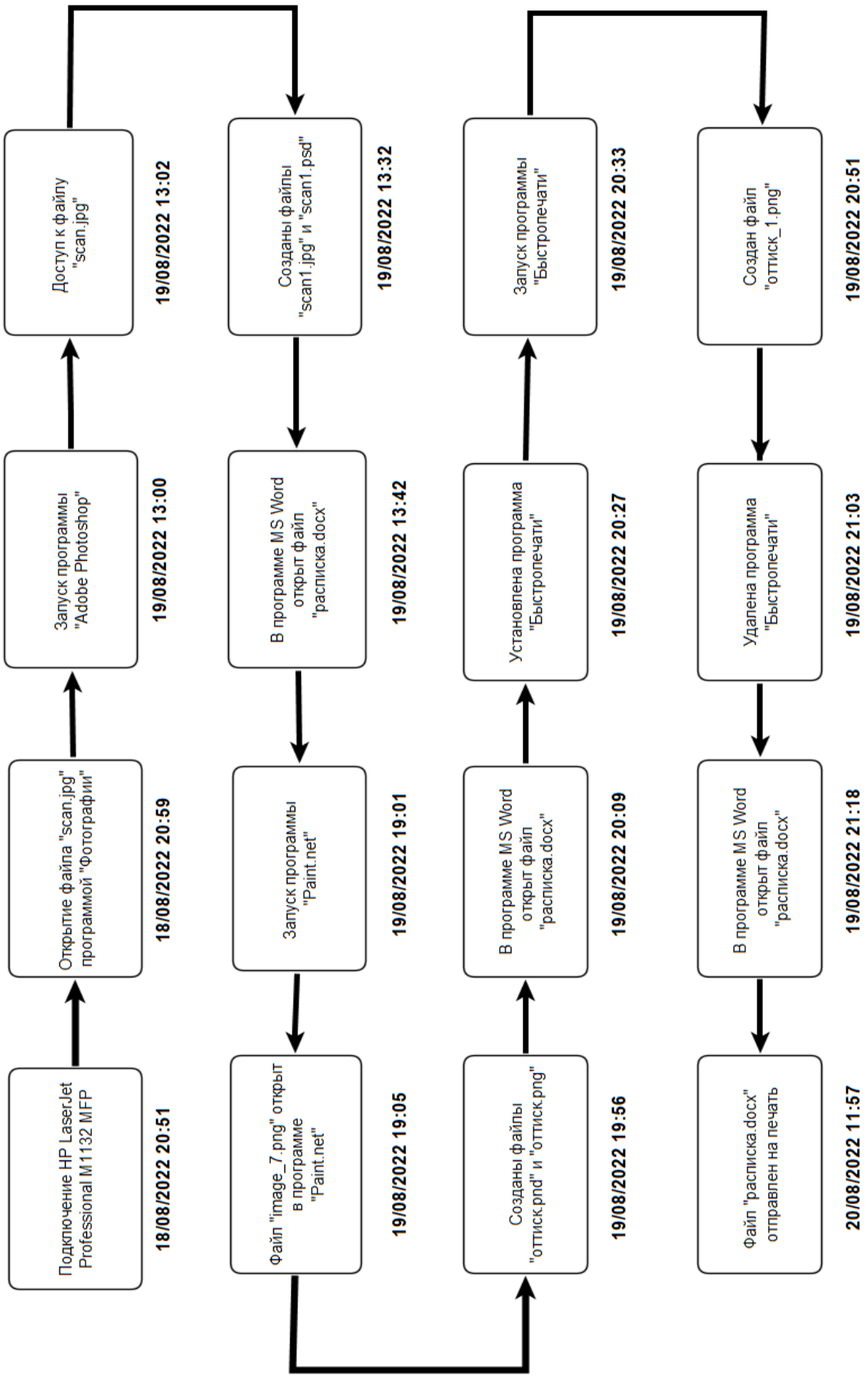


Рис. 6. Временная шкала, отражающая последовательность подготовки документа

Таким образом, предложенные методические рекомендации способствуют проведению всестороннего исследования по выявлению и анализу цифровых следов фальсификации документов методом компьютерного монтажа, а также восстановлению хронологии событий в компьютерной системе. Предложена классификация следов подготовки документов на следы работы с изображениями, следы работы с текстом, следы работы с графическими редакторами и следы подключения периферийных устройств. Указанная классификация позволит эффективно планировать проведение исследований и последующее упорядочение полученных результатов.

Список источников

1. Купин А.Ф. Установление факта компьютерного монтажа документа методами судебной экспертизы / А.Ф. Купин, А.С. Коваленко, Е.К. Сорокина // Дискуссионные вопросы теории и практики судебной экспертизы : материалы IV Международной научно-практической конференции. – Москва, 2021. – С. 354–360.

2. Практические основы компьютерно-технической экспертизы : учебно-методическое пособие / А.Б. Нехорошев, М.Н. Шухнин, И.Ю. Юрин, А.Н. Яковлев. – Саратов : Научная книга, 2007. – 262 с.

3. Larry E. Daniel. Digital Forensics for Legal Professionals / Larry E. Daniel, Lars E. Daniel. – Elsevier, 2012. – 330 с.

4. Shaaban A. Practical Windows Forensics / A. Shaaban, K. Sapronov. – Packt Publishing, 2016. – 314 с.

References

1. Kupin A.F., Kovalenko A.S., Sorokina E.K. The Fact of Computer Modified of the Document by Methods of Digital Forensics. *Discussion Issues in the Theory and Practice of Forensic Examination. Materials of the IV International Scientific and Practical Conference.* Moscow, 2021, pp. 354–360. (In Russian).

2. Nekhoroshev A.B., Shukhnin M.N., Yurin I.Yu., Yakovlev A.N. Practical Foundations of Digital Forensics. Saratov, Nauchnaya kniga Publ., 2007. 262 p.

3. Larry E. Daniel, Lars E. Daniel. Digital Forensics for Legal Professionals. Elsevier, 2012. 330 с.

4. Shaaban A., Sapronov K. Practical Windows Forensics. Packt Publishing, 2016. 314 с.

Информация об авторе

Коваленко Анна Сергеевна –
ассистент кафедры цифровой криминалистики

Information about the Author

Kovalenko Anna Sergeevna –
Assistant of the Chair of Digital Forensic Science

Статья поступила в редакцию 19.10.2023; одобрена после рецензирования 19.11.2023; принята к публикации 20.11.2023.
The article was submitted 19.10.2023; approved after reviewing 19.11.2023; accepted for publication 20.11.2023.