БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2022. – № 2 (105). – 21–33

АВТОМАТИЗАЦИЯ И УПРАВЛЕНИЕ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ И ПРОИЗВОДСТВАМИ

УДК 004 DOI: 10.17212/2782-2230-2022-2-21-33

ПРИМЕНЕНИЕ АВТОМАТИЗИРОВАННЫХ СИСТЕМ В КОМПЬЮТЕРНОЙ КРИМИНАЛИСТИКЕ*

Ю.В. ГРИШИН[1], А.В. ИВАНОВ[2], Н.Е. КАРПОВА[3], А.В. ЧУВАКОВ[4]

[1] *443100, РФ, г. Самара, ул. Молодогвардейская, 244, Самарский государственный технический университет, аспирант кафедры «Электронные системы и информационная безопасность». E-mail: yurikg101@gmail.com*
[2] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, кандидат технических наук, заведующий кафедрой защиты информации. E-mail: andrej.ivanov@corp.nstu.ru*
[3] *443100, РФ, г. Самара, ул. Молодогвардейская, 244, Самарский государственный технический университет, кандидат технических наук, заместитель заведующего кафедрой «Электронные системы и информационная безопасность». E-mail: annuin@mail.ru*
[4] *443100, РФ, г. Самара, ул. Молодогвардейская, 244, Самарский государственный технический университет, кандидат химических наук, доцент кафедры «Электронные системы и информационная безопасность». E-mail: avch2105@gmail.com*

Стремительное развитие и распространение новых информационных и телекоммуникационных технологий приобретает сегодня характер глобальной информационной революции, которая оказывает возрастающее влияние на политику, экономику, управление, финансы, науку, культуру и другие сферы жизнедеятельности общества в рамках национальных границ и в мире в целом. Этим пользуются не только добросовестные пользователи коммуникационных сетей, но и злоумышленники, преследующие различные противоправные цели: личное обогащение, дискредитацию граждан и государственных органов, распространение нелегальной информации, идей терроризма и экстремизма. Также отмечается стремительный рост новых видов преступлений, связанных с применением информационных систем. Всё это требует создания нового инструментария компьютерной криминалистики (форензика), который способен обработать большое количество информации и помочь в выявлении, раскрытии и расследовании преступлений. В статье проанализированы направления современного развития автоматизации поиска и анализа криминалистически значимой информации. Рассмотрены различные виды электронных следов по разным видам преступлений. Предложены новые формы использования ряда элементов искусственного интеллекта и применение математического аппарата в рамках автоматизации экспертных систем для получения необходимых доказательств по соответствующим уголовным делам. Предложена рекоменда-

* Статья получена 20 апреля 2022 г.

тельная система, которая с помощью многофакторного анализа позволит сформировать «портрет» личности на основании данных, содержащихся на электронных носителях пользователя.

Ключевые слова: компьютерная криминалистика, форензика, искусственный интеллект, машинное обучение, математический аппарат, компьютерная судебная экспертиза, электронный след

ВВЕДЕНИЕ

Автоматизация поиска и анализа криминалистически значимой информации – проблема достаточно актуальная сегодня. На сегодняшний момент информационно-телекоммуникационное пространство не является отдельной сферой деятельности, а интегрировано в повседневную жизнь каждого человека. Соответственно, значимость информационных (электронных) следов сегодня не меньшая, а при расследовании отдельных видов преступлений и бóльшая, чем значимость следов материальных. Приходится констатировать, что криминал пока еще явно опережает правоохранительные органы в освоении современных информационных технологий.

В настоящее время с внедрением цифровых технологий во все сферы человеческой деятельности имеет смысл говорить уже не столько об автоматизации, сколько о цифровизации и информатизации работы экспертов, специалистов, криминалистов.

Остро ощущается потребность в разработке автоматизированных программных средств для анализа информационных (электронных) следов. Существует огромный сегмент программных средств, затрагивающих автоматизацию оформительской части (набор и форматирование текста заключения, подготовка иллюстративного материала). Указанные средства уже давно вошли в повседневную практику и уже не воспринимаются как средства автоматизации. Также существует множество информационных систем, позволяющих фиксировать и обрабатывать экспериментальные данные, так называемые «автоматизированные информационно-поисковые системы». Функционирование автоматизированных информационно-поисковых систем основано на принципе сопоставления полученного результата с имеющимися сведениями в базе данных и позволяет эффективно решать экспертные задачи различного характера: идентификационные, классификационные, диагностические [7].

Сегодня, в век больших вычислительных мощностей, имеется тенденция к созданию систем на основе искусственных нейронных сетей. Это направление автоматизации выходит на новый виток развития, и в ближайшее время

именно в этом направлении следует ожидать новых решений в области цифровой криминалистики.

Автоматизированные системы, включая подходы к машинному обучению и системам на основе искусственных нейронных сетей (но не ограничиваясь ими), разрабатываются для того, чтобы помочь людям более эффективно и продуктивно находить ценную информацию в огромных объемах информации. Однако хочется подчеркнуть, что автоматические системы всё же подразумевают непосредственное участие человека в принятии конечного решения. Поэтому оценка отчетов автоматизированных систем или набора предложенных решений и формулирование вывода по-прежнему является задачей человека.

1. ЦИФРОВАЯ КРИМИНАЛИСТИКА

Термин «форензика» образовался от латинского слова *foren*, что означает речь перед форумом, то есть судебные дебаты или выступление перед судом. Этоь термин является сокращением от словосочетания *forensic science* (судебная наука). В русском языке это понятие чаще называют криминалистикой, а слово «форензика» закрепилось за компьютерной ее частью.

Форензика (компьютерная криминалистика) – прикладная наука о раскрытии и расследовании преступлений, которые связаны с компьютерной информацией, а также о методах получения и исследования доказательств, которые имеют форму компьютерной информации, и о применяемых для этого технических средствах.

Перед экспертами-криминалистами ставятся следующие задачи: восстановить хронологию (*timeline*) событий; собрать артефакты (оставшиеся следы событий); провести поиск криминалистически значимой информации и т. д. Также отдельным пунктом стоит задача формирования экспертного заключения, к примеру, для судебных органов или иных компетентных в расследовании инцидентов структур.

Криминалистический процесс, который проводят специалисты и эксперты, принято делить на четыре этапа:

1) сбор информации;

2) исследование (извлечение / считывание информации с носителей, декодирование);

3) анализ (избранная информация анализируется для получения ответов на вопросы, поставленные перед экспертом или специалистом);

4) представление (оформление результатов исследования и анализа в установленной законом и понятной неспециалистам форме).

Компьютерный криминалист вполне может обойтись без специальной криминалистической техники. Компьютер сам по себе – достаточно универсальный инструмент. Среди многообразного периферийного оборудования и программного обеспечения найдутся все необходимые для исследования функции. Некоторые программные инструменты можно легко создать или модифицировать своими руками. Однако специальная техника и специализированное программное обеспечение сильно облегчают работу.

В отношении сбора и исследования информации существует большое количество аппаратно-программных комплексов и программ, автоматизированных в той или иной степени. Однако на третьем этапе избранная информация анализируется для получения ответов на вопросы, поставленные перед экспертом или специалистом. В связи с возрастающим объемом информации, хранящейся на электронных устройствах, увеличивается время на анализ и обработку данных. Теперь большую часть времени в криминалистическом процессе занимает именно анализ больших объемов данных (просмотр журналов и изображений, чтение документов).

В результате информационной перегрузки эти специалисты принимают решения без достаточных механизмов поддержки, увеличивая риск неправильных выводов. Огромные массивы цифровой информации привели к возникновению автоматизированных систем поиска и анализа информации. Это направление является достаточно молодым относительно традиционных видов криминалистических исследований, но одним из самых актуальных в настоящий момент. Погоня за преступниками в виртуальном пространстве по оставленным ими информационным следам имеет мало общего с богатейшим опытом работы оперативно-разыскных служб.

2. СЛОЖНОСТИ ПРИ РАЗРАБОТКЕАВТОМАТИЗИРОВАННЫХ СИСТЕМ АНАЛИЗА

Здесь на первый план исследований и разработок выходят не только проблемы чисто технического плана, но и вопросы обеспечения правового статуса тех сведений криминалистического характера, которые были получены с помощью элементов искусственного интеллекта различного вида. При разработке соответствующих алгоритмов и информационных технологий, в том числе с использованием элементов искусственного интеллекта, необходимо обеспечить применение средств контроля за сохранением правового статуса промежуточных и итоговых результатов обработки информации.

Важно обратить внимание на ряд новых аспектов применения в системе компьютерной криминалистики элементов искусственного интеллекта, которые создаются для обработки информации без участия человека.

По нашему мнению, такие результаты для уголовного судопроизводства в рамках действующего законодательства неприменимы, поскольку их невозможно проверить и оценить в рамках требований, предусмотренных ст. 17, 87 и 88 УПК РФ [2].

3. ЭЛЕКТРОННЫЕ СЛЕДЫ НА НОСИТЕЛЯХ ИНФОРМАЦИИ

Развитие информационных технологий обусловливает образование большого количества электронных следов в различных электронных устройствах, компьютерных сетях и элементах их инфраструктуры, которые необходимо использовать для установления обстоятельств совершенного криминального деяния и причастного к нему лица [1]. Эти следы имеют отношение не только к киберпреступлениям (взлом киберсистем, неправомерный доступ к информации, использование вредоносных программ), но и к любому другому виду преступлений.

Электронные следы – это информация, зафиксированная в цифровом формате, содержащаяся в цифровых устройствах и на различных носителях информации, которая может быть связана с событием преступления, позволяющая установить обстоятельства совершенного преступления и преступника.

Наиболее распространенными устройствами, содержащими электронные следы преступления, являются мобильные телефоны, смартфоны, стационарные компьютеры, ноутбуки, планшеты, различные электронные устройства (электронные часы, пульсометры, шагомеры и пр.) и т. д.

Далее рассмотрим некоторые виды преступлений и попробуем определить, какие электронные следы могут содержаться на устройствах, изъятых в ходе оперативно-разыскных мероприятий и следственных действий.

Так, например, устройства, изъятые по делу, связанному с незаконным изготовлением оружия (ст. 223 УК РФ), могут содержать следующие электронные следы (рис. 1): сведения об истории посещения сети Интернет (тематические форумы, магазины), электронная переписка, литература, схемы и фотографии. Также история посещения сети Интернет и электронная переписка могут содержать в себе ссылки на изображения и документы и сами изображения и документы.

Аналогичные категории электронных следов можно представить и для других дел. Например, для дел, связанных с незаконным хранением растений, содержащих наркотические средства (рис. 2) (ст. 228.1 УК РФ), или для дел, связанных с публичными призывами к осуществлению экстремистской деятельности (рис. 3) (ст. 280 УК РФ).

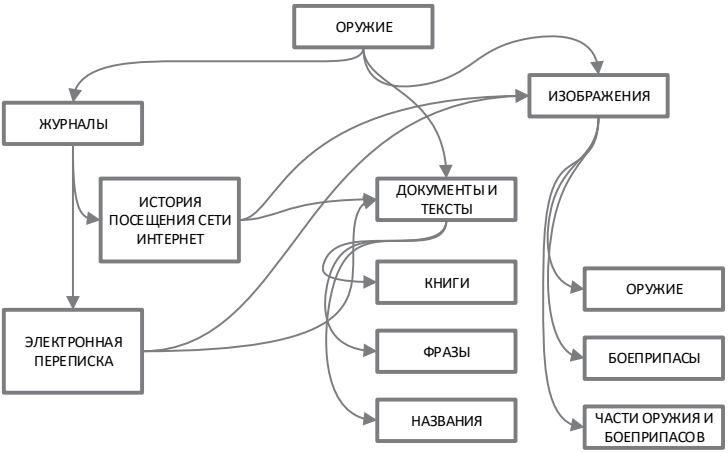

Рис. 1. Электронные следы по категориям преступлений, связанных с оборотом, изготовлением и использованием оружия

Fig. 1. Electronic traces by categories of crimes related to trafficking, manufacture and use of weapons

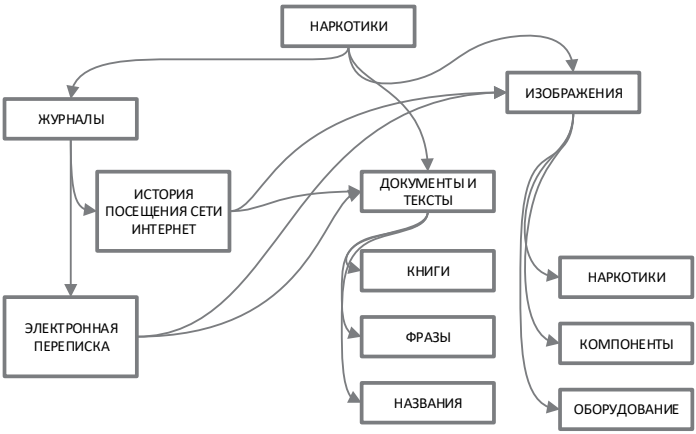

Рис. 2. Электронные следы по категориям преступлений, связанных с оборотом и изготовлением наркотических средств

Fig. 2. Electronic traces by categories of crimes related to trafficking and manufacture of narcotic drugs

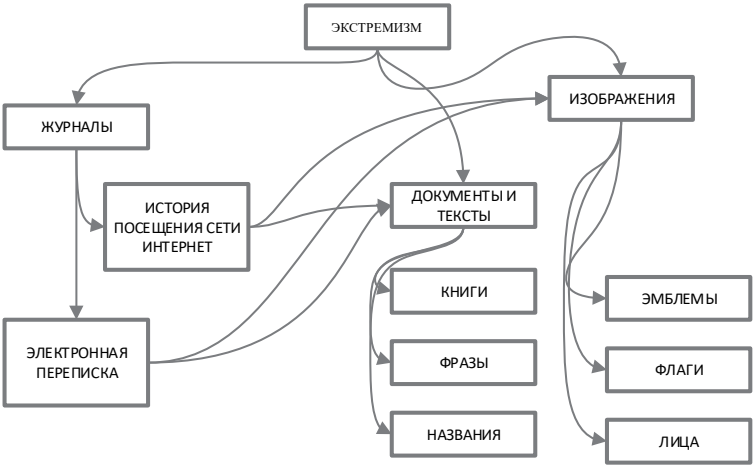

Рис. 3. Электронные следы по категориям преступлений, связанных с экстремистской деятельностью

Fig. 3. Electronic traces by categories of crimes related to extremist activity

Таким образом среди электронных следов необходимо искать документы, фразы, названия соответствующих тематик, ссылки на тематические сайты и электронную переписку, которая может содержать ранее указанные электронные следы. Данный набор электронных следов не является исчерпывающим.

4. МОДЕЛЬ РЕКОМЕНДАТЕЛЬНОЙ СИСТЕМЫ

В обработке больших массивов данных помогла бы автоматизированная система, поддерживающая некий криминалистический анализ, для которого входными данными были бы различные электронные следы, а на выходе формировался бы некоторый криминалистический портрет личности. В предложенной автоматизированной системе предлагается провести анализ данных (цифровых следов) на наличие определенных следов, характеризующих личность (заинтересованность в определенной темнике). Примерный алгоритм работы системы приведен на рис. 4.

На первом этапе происходит подготовка исходных данных и сортировка их по типу. На втором этапе с применением математического аппарата (обработка журналов событий), методов машинного обучения относительно текстов и документов и с использованием искусственных нейронных сетей для распознавания изображений будет формироваться выборка данных. Данным

будет

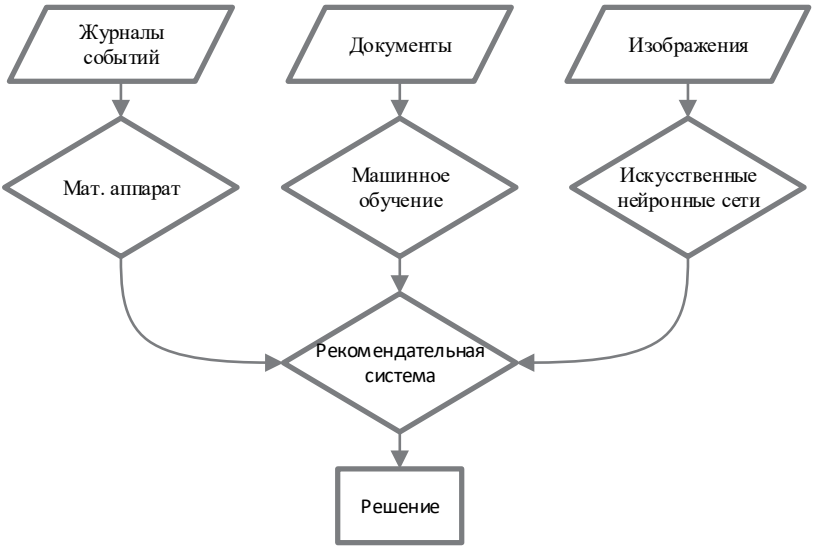

Рис. 4. Структурная схема рекомендательной системы

Fig. 4. Block diagram of the recommendation system

присвоен некий маркер (определение категории). На третьем же этапе с помощью рекомендательной системы многофакторного анализа будет дана оценка, с помощью которой можно будет выделить некоторые цифровые следы, важные для расследуемого дела. Результат может быть представлен в виде отчета, который может содержать обобщенные графики и таблицы, а также набор исходных данных с присвоенным маркером.

ЗАКЛЮЧЕНИЕ

Предложенная модель рекомендательной системы может быть использована в разработке инструмента для криминалистического анализа электронных следов и может масштабироваться. Могут добавляться категории расследуемых дел и может меняться набор входных данных для анализа электронных следов, изъятых из различных устройств. Однако оценка отчетов автоматизированных систем или набора предложенных решений и формулирование вывода является задачей эксперта. Рекомендательная система лишь только указывает на электронные следы, на которые нужно обратить внимание.

СПИСОК ЛИТЕРАТУРЫ

1. *Бессонов А.А.* О некоторых возможностях современной криминалистики в работе с электронными следами // Вестник Университета имени О.Е. Кутафина (МГЮА). – 2019. – № 3 (55). – С. 46–52. – DOI: 10.17803/2311-5998.2019.55.3.046-052.

2. *Волынский А.Ф., Прорвич В.А.* Актуальные проблемы создания инструментария компьютерной криминалистики по преступлениям в сфере цифровой экономики и финансов // Уголовный процесс и криминалистика: теория, практика, дидактика: сборник материалов VI Всероссийской научно-практической конференции (Рязань, 16 декабря 2020 года). – Рязань, 2021. – С. 67–74.

3. *Дяблова Ю.Л.* Криминалистика будущего – цифровая криминалистика? // Актуальные проблемы криминалистики и судебной экспертизы: материалы Международной научно-практической конференции (12 марта 2021 г.). – Иркутск, 2021. – С. 89–92.

4. *Кустов А.М.* «Цифровая криминалистика» или «цифровые технологии в криминалистике» // Современные технологии и подходы в юридической науке и образовании: сборник материалов Международного научно-практического форума, Калининград, 27–31 августа 2020 года. – Калининград, 2021. – С. 173–181.

5. *Михайлов М.А.* Возможности поиска электронных следов и их использование в установлении обстоятельств события, требующего расследования // Уголовное производство: процессуальная теория и криминалистическая практика: материалы VII Международной научно-практической конференции, Алушта, 25–26 апреля 2019 г. – Алушта, 2019. – С. 64–67.

6. *Savel'eva M.V., Smushkin A.B., Potapova N.L.* Innovative approaches to criminalistics // Journal of Siberian Federal University. Humanities and Social Sciences. – 2021. – Vol. 14, N 5. – P. 718–723. – DOI: 10.17516/1997-1370-0754.

7. *Себякин А.Г.* Пути автоматизации экспертиз: от правовой кибернетики до цифровой криминалистики // ГлаголЪ правосудия. – 2018. – № 4 (18). – С. 53–55.

8. *Serebrennikova A.V.* Digital forensics: the genesis of the concept // Colloquium-journal. – 2020. – N 21 (73), pt. 2. – P. 60–62. – DOI: 10.24411/2520-6990-2020-12102.

9. *Bollé T., Casey E., Jacquet M.* The role of evaluations in reaching decisions using automated systems supporting forensic analysis // Forensic Science International: Digital Investigation. – 2020. – Vol. 34. – P. 301016. – DOI: 10.1016/j.fsidi.2020.301016.

10. Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001г. №174-ФЗ (в последней ред. ФЗ от 6.12.07. №335-ФЗ) //Собрание законодательства РФ. 2001. – №52 (ч.1).–Ст.4921; 2007. – №16. – Ст. 1827.

11. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (в последней ред. ФЗ от 06.12.07 № 335-ФЗ) // Собрание законодательства Российской Федерации. – 1996. – № 25. – Ст. 2954; 2007. – № 16. – Ст. 1826.

12. *Ходоева Э.Д.* Понятие и способы сокрытия электронных следов преступления // Global and Regional Research. – 2020. – Т. 2, № 2. – С. 399–405.

Гришин Юрий Валерьевич, аспирант кафедры «Электронные системы и информационная безопасность» Самарского государственного технического университета. Основное направление научных исследований – применение методов многофакторного анализа в форензике. E-mail: yurikg@gmail.com

Иванов Андрей Валерьевич, кандидат технических наук, заведующий кафедрой защиты информации Новосибирского государственного технического университета. Область научных интересов – обработка звука от шума, техническая защита информации от утечки по каналам связи. E-mail: andrej.ivanov@corp.nstu.ru

Карпова Надежда Евгеньевна, кандидат технических наук, заместитель заведующего кафедрой «Электронные системы и информационная безопасность» Самарского государственного технического университета. Область научных интересов – автоматизация процессов, нейронные сети, техническая защита информации от утечки по каналам связи. E-mail: annuin@mail.ru

Чуваков Александр Владимирович, кандидат химических наук, доцент кафедры «Электронные системы и информационная безопасность» Самарского государственного технического университета. Область научных интересов – автоматизация процессов, нейронные сети, техническая защита информации от утечки по каналам связи. E-mail: avch2105@gmail.com

DOI: 10.17212/2782-2230-2022-2-21-33

The use of automated systems in computer forensics*

Y.V. Grishin[1], A.V. Ivanov[2], N.E. Karpova[3], A.V. Chuvakov[4]

[1] *Samara State Technical University, 244 Molodogvardeyskaya Street, Samara, 443100, Russian Federation, graduate student of the Electronic Systems and Information Security Department. E-mail: yurikg101@gmail.com*
[2] *Novosibirsk State Technical University, 20 Karl Marx Prospekt, Novosibirsk, 630073, Russian Federation, candidate of technical sciences, head of the Information Security Department. E-mail: andrej.ivanov@corp.nstu.ru*
[3] *Samara State Technical University, 244 Molodogvardeyskaya Street, Samara, 443100, Russian Federation, candidate of technical sciences, associate head of the Electronic Systems and Information Security Department. E-mail: annuin@mail.ru*
[4] *Samara State Technical University, 244 Molodogvardeyskaya Street, Samara, 443100, Russian Federation, candidate of chemical sciences, associate professor of the Electronic Systems and Information Security Department. E-mail: avch2105@gmail.com*

The rapid development and spread of new information and telecommunication technologies is acquiring the character of a global information revolution today, which has an increasing impact on politics, economics, management, finance, science, culture and other spheres of society within national borders and in the world as a whole. This is used not only by conscientious users of communication networks, but also by malefactors pursuing various illegal goals – personal enrichment, discrediting citizens and state bodies, spreading illegal information, ideas of terrorism and extremism. There is also a rapid growth of new types of crimes related to the use of information systems. All this requires the creation of new computer forensics tools (forensics), which is able to process a large amount of information and help in the identification, disclosure and investigation of crimes. The article analyzes the directions of modern development of automation of search and analysis of criminally significant information. Various types of electronic traces for different types of crimes are considered. New forms of using a number of elements of artificial intelligence and the use of mathematical apparatus within the automation of expert systems to obtain the necessary evidence in relevant criminal cases are proposed. A recommendation system is proposed, which, with the help of multifactor analysis, will allow to form a "portrait" of a person based on the data contained on the user's electronic media.

Keywords: computer forensics, forensics, artificial intelligence, machine learning, mathematical apparatus, computer forensic examination, electronic trace

REFERENCES

1. Bessonov A.A. O nekotorykh vozmozhnostyakh sovremennoi kriminalistiki v rabote s elektronnymi sledami [On some possibilities of modern forensic science in working with electronic traces]. *Vestnik Universiteta imeni O.E. Kutafina*

* *Received 20 April 2022.*

(MGYuA) = Courier of Kutafin Moscow State Law University (MSAL), 2019, no. 3 (55), pp. 46–52. DOI: 10.17803/2311-5998.2019.55.3.046-052.

2. Volynskii A.F., Prorvich V.A. [Actual problems of creating computer criminalistics tools for crimes in the field of digital economy and finance]. *Ugolovnyi protsess i kriminalistika: teoriya, praktika, didaktika* [Criminal process and criminalistics: theory, practice, didactics]. Collection of materials of the VI All-Russian Scientific and Practical Conference, Ryazan, December 16, 2020, pp. 67–74. (In Russian).

3. Dyablova Yu.L. [Criminalistics of the future – digital criminalistics?]. *Aktual'nye problemy kriminalistiki i sudebnoi ekspertizy* [Actual problems of criminalistics and forensic examination]. Materials of the International Scientific and Practical Conference, Irkutsk, March 12, 2021, pp. 89–92. (In Russian).

4. Kustov A.M. ["Digital criminalistics" or "digital technologies in criminalistics"]. *Sovremennye tekhnologii i podkhody v yuridicheskoi nauke i obrazovanii* [Modern technologies and approaches in legal science and education]. Collection of materials of the International Scientific and practical Forum, Kaliningrad, August 27–31, 2020. Kaliningrad, 2021, pp. 173–181. (In Russian).

5. Mikhailov M.A. [The possibilities of searching for electronic traces and their use in establishing the circumstances of an event requiring investigation]. *Ugolovnoe proizvodstvo: protsessual'naya teoriya i kriminalisticheskaya praktika* [Criminal proceedings: procedural theory and forensic practice]. Materials of the VII International Scientific and Practical Conference], Alushta, April 25–26, 2019, pp. 64–67. (In Russian).

6. Savel'eva M.V., Smushkin A.B., Potapova N.L. Innovative approaches to criminalistics. *Journal of Siberian Federal University. Humanities and Social Sciences*, 2021, vol. 14, no. 5, pp. 718–723. DOI: 10.17516/1997-1370-0754.

7. Sebyakin A.G. Puti avtomatizatsii ekspertiz: ot pravovoi kibernetiki do tsifrovoi kriminalistiki [Ways of automation expertise: from legal cybernetics to digital criminalistics]. *Glagol" pravosudiya = Verb of Justice*, 2018, no. 4 (18), pp. 53–55.

8. Serebrennikova A.V. Digital forensics: the genesis of the concept. *Colloquium-journal*, 2020, no. 21 (73), pt. 2, pp. 60–62. DOI: 10.24411/2520-6990-2020-12102.

9. Bollé T., Casey E., Jacquet M. The role of evaluations in reaching decisions using automated systems supporting forensic analysis. *Forensic Science International: Digital Investigation*, 2020, vol. 34, p. 301016. DOI: 10.1016/j.fsidi.2020.301016.

10. Ugolovno-processual'nyj kodeks Rossijskoj Federacii ot 18 dekabrya 2001g. №174-FZ (v poslednej red. FZ ot 6.12.07. №335-FZ) [Criminal Procedure Code of the Russian Federation No. 174-FZ of December 18, 2001 (in the latest

edition. Federal Law of 6.12.07. No. 335-FZ)]. Sobranie zakonodatel'stva RF = Collection of legislation of the Russian Federation. 2001. – No. 52 (part 1). – St.4921; 2007. – № 16. – Article 1827.

11. Criminal Code of the Russian Federation No. 63-FZ of June 13, 1996 (in the latest edition. Federal Law No. 335-FZ dated 06.12.07). *Sobranie zakonodatel'stva Rossiiskoi Federatsii = Collection of the legislation of the Russian Federation*, 1996, no. 25, art. 2954; 2007, no. 16, art. 1826. (In Russian).

12. Khodoeva E.D. Ponyatie i sposoby sokrytiya elektronnykh sledov prestupleniya [Concept and methods of covering electronic trains of crime]. *Global and Regional Research*, 2020, vol. 2, no. 2, pp. 399–405. (In Russian).

Для цитирования:

Применение автоматизированных систем в компьютерной криминалистике / Ю.В. Гришин, А.В. Иванов, Н.Е. Карпова, А.В. Чуваков // Безопасность цифровых технологий. – 2022. – № 2 (105). – С. 21–33. – DOI: 10.17212/2782-2230-2022-2-21-33.

For citation:

Grishin Yu.V., Ivanov A.V., Karpova N.E., Chuvakov A.V. Primenenie avtomatizirovannykh sistem v komp'yuternoi kriminalistike [The use of automated systems in computer forensics]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2022, no. 2 (105), pp. 21–33. DOI: 10.17212/2782-2230-2022-2-21-33.