УДК 343.98 **DOI: 10.34670/AR.2022.69.81.029**

Инновационные технические средства и оборудование в решении экспертных задач судебной компьютерно-технической экспертизы

Хахина Анна Михайловна

Доктор технических наук, профессор,
Санкт-Петербургский политехнический университет Петра Великого,
195251, Российская Федерация, Санкт-Петербург,
ул. Политехническая, 29;
e-mail: anna-hahina@mail.ru

Ермолаева Александра Сергеевна

Студент,
Санкт-Петербургский политехнический университет Петра Великого,
195251, Российская Федерация, Санкт-Петербург,
ул. Политехническая, 29;
e-mail: reallex@icloud.com

Молодых Елизавета Игоревна

Студент,
Санкт-Петербургский политехнический университет Петра Великого,
195251, Российская Федерация, Санкт-Петербург,
ул. Политехническая, 29;
e-mail: hahina_liza2001@mail.ru

Аннотация

С развитием и широким распространением цифровых и компьютерных технологий частым проявлением в среде преступности стали различного рода устройства и программы. Получение улик, путем извлечения информации с носителя, установления фактического состояния устройства, подбор паролей, анализ программ, стало неотъемлемой частью криминалистики. Подобные исследования невозможны без качественных экспертных знаний в области информатики, кибернетики и собственных экспертных знаний и методик. В статье рассматривают понятие и виды судебной компьютерно-технической экспертизы. Даны основные определения, приведена классификация такого рода судебно-технической экспертизы, как компьютерной. В статье рассматриваются инновационные технические средства и оборудование в компьютерно-технической экспертизе. Наиболее подробно рассмотрены такие средства, как аппаратные и программные комплексы. Особое внимание уделяется использованию результатов компьютерно-технической экспертизы в решении задач судопроизводства. Представлены инновационные технические средства, которые являются неотъемлемой частью всего процесса исследования судебной компьютерно-

технической экспертизы, что позволяет ускорить процесс исследования, тем самым способствуя раскрытию преступлений. Показана важность использования перечисленного оборудования для решения задач, которые поставлены перед судебным экспертом, от исследования, которого зависит результат судопроизводства. Выявлены перспективы развития и отражен процесс совершенствования всех названных технических средств.

Для цитирования в научных исследованиях

Хахина А.М., Ермолаева А.С., Молодых Е.И. Инновационные технические средства и оборудование в решении экспертных задач судебной компьютерно-технической экспертизы // Вопросы российского и международного права. 2022. Том 12. № 6А. С. 218-224. DOI: 10.34670/AR.2022.69.81.029

Ключевые слова

Экспертиза, комплекс, криминалистика, компьютер, оборудование, инновации, лаборатория.

Введение

С развитием и широким распространением цифровых и компьютерных технологий частым проявлением в среде преступности стали различного рода устройства и программы. Получение улик, путем извлечения информации с носителя, установления фактического состояния устройства, подбор паролей, анализ программ, стало неотъемлемой частью криминалистики. Подобные исследования невозможны без качественных экспертных знаний в области информатики, кибернетики и собственных экспертных знаний и методик.

Актуальность статьи обусловлена тем, что развитие компьютерных и новых технологий очень стремительны и требуют для своего исследования качественный набор специальных средств и оборудований.

Основная часть

Причины развития судебной компьютерно-технической экспертизы обусловлены научно-техническим прогрессом и развитием информационных технологий. Очевидно, что в ранние годы электронно-вычислительные машины не были распространены среди простого населения в силу дороговизны и массивности их конструкции. С течением времени стали появляться персональные компьютеры и ЭВМ для потребительского рынка, то есть компьютерные технологии стали доступны широкому кругу пользователей. Однако помимо использования компьютеров в целях увеличения продуктивности работы, творчества и науки, компьютеры стали использовать в преступных целях. Так в мире появился еще один вид преступлений, который называется киберпреступлениями. Киберпреступления были направлены не только на мошеннические действия, но и могли покушаться на информацию, в том числе и государственную [Завьялов, 2020].

В России к концу 20 века активно занялись вопросами безопасности информации и высоких технологий. В 1999 году на базе Экспертно-криминалистический центра Министерства внутренних дел был создан отдел компьютерных экспертиз и научно-исследовательская лаборатория. В дальнейшие годы при Российском федеральном центре судебной экспертизы появилась специализированная лаборатория судебной компьютерно-технической экспертизы и

информационных технологий, а перечне специальностей ГСЭУ Минюста появилась специальность «Исследование информационных компьютерных средств»[1].

Судебная компьютерная техническая экспертиза относится к классу инженерно-технических экспертиз при этом является самостоятельным родом.

Это относительный новый вид экспертизы, имеющий на данный момент сравнительно узкий теоретический базис. К этому прибавляется факт развития различных способов и приемов, используемые в киберпреступлениях. Однако компьютерная экспертиза развивается и нарабатывает опыт и историю.

Полнота исследований невозможна без применений средств и оборудований. Оборудование современной судебной компьютерно-технической экспертизы представлены не только компьютерами и устройствами, но также и специальными программами, которые позволяют проводить качественные исследования.

Аппаратное обеспечение судебной компьютерно-технической экспертизы – это набор электронных и механических частей вычислительных устройств. В аппаратное обеспечение судебной компьютерно-технической экспертизы входят:

– Аппаратно-программные комплексы;

– Аппараты для конкретного вида исследования.

На примере аппаратно-программного комплекса UFED 4PC раскроем суть данного средства судебной компьютерно-технической экспертизы. По данным сайта Aimtech.ru UFED 4PC является универсальным средством, оно позволяет извлекать и анализировать данные с носителей информации. Данный аппаратно-програмный комлекс имеет в своей комплектации большой набор инструментов, позволяющие работать с различными видами объектов судебной компьютерно-технической экспертизы. Состав аппаратно-программного комплексы UFED 4PC включает в себя[2]: ПО UFED Physical Analyzer (входит в комплект Ultimate); ПО UFED Logical Analyzer; ПО UFED Reader; ПО UFED Phone Detective; переходник UFED; кейс для переноски UFED; комплект кабелей и разъемов; кард-ридер UFED; адаптер Multi SIM; карты для клонирования ID SIM/MicroSIM/NanoSIM; кабель питания телефона; щетка для очистки разъемов телефона; ремень с липучкой; флеш-накопитель USB; удлинитель USB; USB-кабель питания для адаптера UFED; UFED Camera (входит в комплект Ultimate).

Еще одной вариацией аппаратно-программного обеспечения являются специализированные переносные лаборатории. Специализированння переносная лаборатория RoadMASSter-3 X2 Forensic или RM3. Ее достоинством является мобильность, с ней можно выехать на место расследования, если объект исследования по различным причинам извлечь и перевезти не представляется возможным. Функционал лаборатории включает в себя копирование данных с различными режимами, анализ данных, стирание данных.[3]

Помимо аппаратно-программных комплексов судебная компьютерно-техническая располагает устройствами, обладающие функционалом по решению конкретной задачи. Они могут как входить в состав аппаратно-программных комплексов, так и использоваться отдельно от них. Примерами таких устройств можно считать: Tableau Forensic Imager TX1 – устройство копирования данных; Tableau Password Recovery – устройство подбора и взлома паролей;

[1] Приказ Минюста России от 14.05.2003 №114 «Об утверждении Перечня родов (видов) экспертиз выполняемых в ГСЭУ Минюста РФ

[2] UFED 4PC // Целевые технологии URL: https://forensictools.com.ua/home/roadmasster-3-x2-forensic-.html

[3] EPOS Forensic tools URL: https://forensictools.com.ua/home/roadmasster-3-x2-forensic-.html

Logicub Talon Ultimate – устройство для копирования жестких дисков.

Следующей большой группой средств судебной компьютерно-технической экспертизы следует считать программные комплексы. Они работают совместно с аппаратными комплексами. В настоящее есть большое разнообразие программ, используемые криминалистами. Самыми известными из них являются: BelkaSoft Evidence Center X; Blacklight Cellebrite; Elcomsoft; Мобильный криминалист.

BelkaSoft Evidence Center X – это программный комплекс от компании ООО «Белкасофт». Данный продукт используется в расследовании преступлений, разведке и расследовании внутренних инцидентов в компаниях[4]. Данная программа входит в Реестр российских программ по Приказу Минкомсвязи РФ от 07.12.2017 №680, Приложение 1, №пп.134, реестровый № 4103. Заказчиками являются Министерство внутренних дел РФ (ЭКЦ МВД), Управление «К» МВД РФ, Следственный комитет РФ, ФСБ, ФСИН Министерство юстиции, Банк «Петрокоммерц».

Программный комплекс способен работать с информационными объектами, в терминологии Belkasoft они именуются артефактами [АнТЯСОВ, Уфимцев, 2016], извлекать файлы, анализировать файлы подкачки и гибернации, работает с образами дисков.

Blacklight от израильской компании Cellebrite – программа, позволяющая всесторонне анализировать компьютеры, телефоны, планшетные компьютеры под управлениям Mac и Windows. В функционал входит анализ реестра Windows и данных об учетных записях, загрузках, корзине, USB-соединениях и т.п., просмотр истории устройств из теневых копий томов Microsoft. Применяя к техникеApple Blacklight, становится возможным просмотр истории в моментальных снимках Apple File System и резервных копиях Time Machine, отображение и поиск метаданных Spotlight, просмотр сетевых подключений, последних документов, активность пользователь и т.п.

Elcomsoft – российская компания, специализирующаяся на вопросах информационной безопасности и цифровой криминалистики. Elcomsoft Premium Forensic Bundle предлагает эксперту широкий спектр возможностей проведения исследований. С помощью этой программы решаются проблемы восстановления и снятия паролей в большом количестве продуктов, включая учетные записи Windows, приложения Microsoft Office, файлы Adobe PDF, архивы ZIP и RAR[5].

Мобильный криминалист – программное обеспечении для извлечения данных с телефонов и компьютеров. По данным сайта Aimtech Мобильный криминалист имеет широкий набор функций. Это возможность извлекать все данные пользователя, просмотр данных в шестнадцатеричном виде, просмотр веб-страниц, текстовых документов, отслеживания местоположения устройств, загрузка и анализ резервных копий, поиск в словаре устройства, извлечение переписки и т.п.

Заключение

Все перечисленные аппаратные и программные устройства являются неотъемлемой частью всего процесса исследования судебной компьютерно-технической экспертизы. Они заметно упрощают процесс исследования, так как объем исследования компьютеров очень велик, чтобы его можно было охватить исключительно специальными знаниями эксперта.

[4] Belkasoft URL: https://belkasoft.com/ru/company

[5] О компании Элкомсофт. URL: https://www.elcomsoft.ru/company.html

От того насколько эффективно работает оборудование и специальное программное обеспечение зависит правильно выполненная экспертиза. В настоящее время идет процесс совершенствования всех вышеперечисленных технических средств.

Библиография

1. Антясов И.С., Уфимцев М.С. Программное обеспечение и методы восстановления информации при проведении компьютерных экспертиз // Вестник УрФО. Безопасность в информационной сфере. 2016. № 3 (21). С. 16-23.
2. Завьялов Д.В. Современные возможности судебной компьютерно-технической экспертизы, при расследовании различных видов преступлений // Теория и практика судебной экспертизы. 2020. № 3. С. 89-97.
3. О компании Элкомсофт. URL: https://www.elcomsoft.ru/company.html
4. Приказ Минюста России от 14.05.2003 №114 «Об утверждении Перечня родов (видов) экспертиз выполняемых в ГСЭУ Минюста РФ».
5. Belkasoft. URL: https://belkasoft.com/ru/company
6. EPOS Forensic tools. URL: https://forensictools.com.ua/home/roadmasster-3-x2-forensic-.html
7. UFED 4PC. URL: https://forensictools.com.ua/home/roadmasster-3-x2-forensic-.html
8. Klymchuk M. et al. Evaluation of forensic computer and technical expertise in criminal proceedings //Amazonia Investiga. – 2021. – Т. 10. – №. 38. – С. 204-211.
9. Petrenko V. I. et al. Judicial technical expertise methods for investigation of cybercrimes //IOP Conference Series: Materials Science and Engineering. – IOP Publishing, 2021. – Т. 1069. – №. 1. – С. 012041.
10. Abdusalamovich T. X. Some questions about the role of a forensic expert in investigating computer-related crimes //ACADEMICIA: An International Multidisciplinary Research Journal. – 2021. – Т. 11. – №. 7. – С. 81-84.

Innovative technical means and equipment in solving expert tasks of forensic computer-technical expertise

Anna M. Khakhina

Doctor of Technical Science, Professor,
Peter the Great Saint Petersburg Polytechnic University,
195251, 29, Politekhnicheskaya str., Saint Petersburg, Russian Fedeartion;
e-mail: anna-hahina@mail.ru

Aleksandra S. Ermolaeva

Graduate Student,
Peter the Great Saint Petersburg Polytechnic University,
195251, 29, Politekhnicheskaya str., Saint Petersburg, Russian Fedeartion;
e-mail: reallex@icloud.com

Elizaveta I. Molodykh

Graduate Student,
Peter the Great Saint Petersburg Polytechnic University,
195251, 29, Politekhnicheskaya str., Saint Petersburg, Russian Fedeartion;
e-mail: hahina_liza2001@mail.ru

Abstract

With the development and widespread use of digital and computer technologies, various kinds of devices and programs have become a frequent manifestation in the criminal environment. Obtaining evidence by extracting information from the media, establishing the actual state of the device, guessing passwords, analyzing programs, has become an integral part of forensic science. Such research is impossible without high-quality expert knowledge in the field of informatics, cybernetics and our own expert knowledge and methods. The article considers the concept and types of forensic computer-technical expertise. The main definitions are given the classification of this kind of forensic technical expertise, as a computer one is given. The article deals with innovative technical means and equipment in computer-technical expertise. The most detailed consideration of such tools as hardware and software systems. Particular attention is paid to the use of the results of computer-technical expertise in solving problems of legal proceedings. Innovative technical means are presented, which are an integral part of the entire process of forensic computer-technical examination research, which makes it possible to speed up the research process, thereby contributing to the detection of crimes. The importance of using the listed equipment for solving the tasks assigned to the forensic expert is shown, from the study, which depends on the result of legal proceedings. The development prospects are revealed and the process of improvement of all the named technical means is reflected.

For citation

Khakhina A.M., Ermolaeva A.S., Molodykh E.I. (2022) Innovatsionnye tekhnicheskie sredstva i oborudovanie v reshenii ekspertnykh zadach sudebnoi komp'yuterno-tekhnicheskoi ekspertizy [Innovative technical means and equipment in solving expert tasks of forensic computer-technical expertise]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 12 (6A), pp. 218-224. DOI: 10.34670/AR.2022.69.81.029

Keywords

Expertise, complex, criminalistics, computer, equipment, innovations, laboratory.

References

1. Antyasov I.S., Ufimtsev M.S. (2016) Programmnoe obespechenie i metody vosstanovleniya informatsii pri provedenii komp'yuternykh ekspertiz [Software and methods of information recovery during computer forensics]. *Vestnik UrFO. Bezopasnost' v informatsionnoi sfere* [Bulletin of the Ural Federal District. Security in the information sphere], 3 (21), pp. 16-23.
2. *Belkasoft.* Available at: https://belkasoft.com/ru/company [Accessed 04/04/2022]
3. *EPOS Forensic tools.* Available at: https://forensictools.com.ua/home/roadmasster-3-x2-forensic-.html [Accessed 04/04/2022]
4. *O kompanii Elkomsoft* [About Elcomsoft]. Available at: https://www.elcomsoft.ru/company.html [Accessed 04/04/2022]
5. *Prikaz Minyusta Rossii ot 14.05.2003 №114 «Ob utverzhdenii Perechnya rodov (vidov) ekspertiz vypolnyaemykh v GSEU Minyusta RF»* [Order of the Ministry of Justice of Russia dated May 14, 2003 No. 114 "On approval of the List of genera (types) of examinations performed at the SSEI of the Ministry of Justice of the Russian Federation"].
6. *UFED 4PC.* Available at: https://forensictools.com.ua/home/roadmasster-3-x2-forensic-.html [Accessed 04/04/2022]
7. Zav'yalov D.V. (2020) Sovremennye vozmozhnosti sudebnoi komp'yuterno-tekhnicheskoi ekspertizy, pri rassledovanii razlichnykh vidov prestuplenii [Modern possibilities of forensic computer-technical expertise in the investigation of various types of crimes]. *Teoriya i praktika sudebnoi ekspertizy* [Theory and practice of forensic expertise], 3, pp. 89-97.
8. Klymchuk, M., Marko, S., Priakhin, Y., Stetsyk, B., & Khytra, A. (2021). Evaluation of forensic computer and technical expertise in criminal proceedings. Amazonia Investiga, 10(38), 204-211.
9. Petrenko, V. I., Bereznitsky, A. S., Ogur, M. G., & Nekrasova, E. A. (2021, March). Judicial technical expertise methods

for investigation of cybercrimes. In IOP Conference Series: Materials Science and Engineering (Vol. 1069, No. 1, p. 012041). IOP Publishing.
10. Abdusalamovich, T. X. (2021). Some questions about the role of a forensic expert in investigating computer-related crimes. ACADEMICIA: An International Multidisciplinary Research Journal, 11(7), 81-84.