**Лабораторная работа №1**

**ФИО**

Харитонов Артем Сергеевич (6114-100503D)

Тудаков Родион Алексеевич (6114-100503D)

**Topic**

Digital Forensics; Cybercrime; Court of Law

**Описание предметной области**

Данный топик относится к области информационной безопасности и управлением доступом в информационных системах.

Цифровая криминалистика DFF (Digital Forensics Framework) — фреймворк для криминалистического анализа, интерфейсы представлены как в виде командной строки, так и GUI. DFF можно использовать для исследования жестких дисков и энергозависимой памяти и создания отчетов о пользовательских и системных действиях.

Киберпреступность (Cybercrime) – это преступная деятельность, в рамках которой используются либо атакуются компьютер, компьютерная сеть или сетевое устройство.  
Суд общей юрисдикции (Court of Law) — это суд, осуществляющий правосудие по гражданским, уголовным делам и делам, возникающим из административных правонарушений, а также иным делам, подсудным судам общей юрисдикции.

**Недостаток (Gap)**

Один из основных недостатков научной проработки области заключается в недостаточности разработки общих стандартов и протоколов для реализации цифровой криминалистики. Это приводит к тому, что специалисты в области цифровой криминалистики работают без четких правил и стандартов, что затрудняет сравнение результатов и поддержку выводов в суде. Кроме того, многие исследования в области цифровой криминалистики фокусируются на разработке новых методов и инструментов, но оставляют за рамками внимания вопросы обоснования и подтверждения достоверности этих методов.

**Идея**

Разработать единый подход к реализации протоколов цифровой криминалистики, учитывая общие стандарты.

**Краткий текст обзора**

Цифровая криминалистика является важной областью в борьбе с киберпреступностью, так как она позволяет проводить расследования и собирать доказательства о преступлениях, совершенных с использованием компьютерных технологий и интернета [1][9][1,2](https://www.zotero.org/google-docs/?WKL6FR). Юридические аспекты цифровой криминалистики и электронных доказательств [7][8][3,4](https://www.zotero.org/google-docs/?LpCkQN) играют важную роль в небезопасном электронном мире, где киберпреступности становятся все более распространенными.

Важным аспектом цифровой криминалистики является использование и критерия доказательной базы [12][5](https://www.zotero.org/google-docs/?lKolIM), которая должна быть надежной и достоверной для подачи в суд материалов о преступлении. В отдельных случаях неправильно использованные доказательства могут быть отклонены судом ввиду их двоякости или же неграмотной трактовки. Правовые аспекты цифровой криминалистики играют важную роль в обеспечении законности при расследовании преступлений, связанных с использованием компьютерных технологий [2][6](https://www.zotero.org/google-docs/?5fAZt6). Одним из ключевых аспектов является соблюдение приватности и защита данных при сборе, анализе и представлении цифровых доказательств в судебном процессе. Существующие законы и нормы не всегда соответствуют современным реалиям цифровой среды, что затрудняет борьбу с киберпреступностью и эффективное использование цифровых доказательств в судебных процессах [3][7](https://www.zotero.org/google-docs/?kESc8x).

Для сбора и анализа цифровых доказательств применяются различные методы и инструменты [5][8](https://www.zotero.org/google-docs/?W7RWs6). Среди них можно выделить программное обеспечение для экспертизы цифровых устройств, специализированные алгоритмы для анализа сетевого трафика и инструменты для восстановления удаленных данных. Методы цифровой криминалистики включают в себя исследование цифровых следов, анализ метаданных, криптоанализ и использование специализированных баз данных. Поддомены цифровой криминалистики на современном этапе развития включают в себя широкий спектр направлений и специализаций [11][9](https://www.zotero.org/google-docs/?rNBJZP). Некоторые из них включают в себя кибербезопасность, цифровой анализ данных, цифровую биометрию, мобильную криминалистику, киберспоры и многое другое.

Для устранения недостатка общих стандартов для реализации цифровой криминалистики важно проводить дальнейшие исследования и разработку общих стандартов, которые были бы приняты сообществом специалистов по цифровой криминалистике и судебной экспертизе. Создание унифицированных процедур и протоколов поможет повысить надежность и достоверность цифровых доказательств, а также обеспечит их лучшую защиту в судебных процессах.

Итак, применение современных методов и инструментов цифровой криминалистики позволяет эффективно бороться с киберпреступностью и обеспечивать справедливость в цифровом мире. Умение проводить качественные цифровые расследования и использовать достоверные доказательства является ключевым элементом в борьбе с преступностью, основанной на использовании современных технологий.

References

[1]

E. Brown, «Digital Forensic and Distributed Evidence», *Advances in Multidisciplinary and scientific Research Journal Publication*, т. 1, сс. 357–362, июл. 2022, doi: [10.22624/AIMS/CRP-BK3-P57](https://doi.org/10.22624/AIMS/CRP-BK3-P57).

[2]

A. Al-Dhaqm *и др.*, «Digital Forensics Subdomains: The State of the Art and Future Directions», *IEEE Access*, т. 9, сс. 152476–152502, 2021, doi: [10.1109/ACCESS.2021.3124262](https://doi.org/10.1109/ACCESS.2021.3124262).

[3]

University Of East London и O. Ay, «Digital Forensics Investigation Jurisprudence: Issues Of Admissibility Of Digital Evidence», *Forensic Leg Investig Sci*, т. 6, вып. 1, сс. 1–8, июл. 2020, doi: [10.24966/FLIS-733X/100045](https://doi.org/10.24966/FLIS-733X/100045).

[4]

K. H. Mohammed, Y. D. Mohammed, и A. A. Solanke, «Cybercrime and Digital Forensics: Bridging the gap in Legislation, Investigation and Prosecution of Cybercrime in Nigeria», *International Journal of Cybersecurity Intelligence & Cybercrime*, т. 2, вып. 1, сс. 56–63, фев. 2019, doi: [10.52306/2578-3289.1014](https://doi.org/10.52306/2578-3289.1014).

[5]

A. Yeboah-Ofori, E. Yeboah-Boateng, и H. Gustav Yankson, «Relativism Digital Forensics Investigations Model: A Case for the Emerging Economies», в *2019 International Conference on Cyber Security and Internet of Things (ICSIoT)*, Accra, Ghana: IEEE, май 2019, сс. 93–100. doi: [10.1109/ICSIoT47925.2019.00023](https://doi.org/10.1109/ICSIoT47925.2019.00023).

[6]

M. Losavio *и др.*, «The juridical spheres for digital forensics and electronic evidence in the insecure electronic world», *Wiley Interdisciplinary Reviews: Forensic Science*, т. 1, с. e1337, май 2019, doi: [10.1002/wfs2.1337](https://doi.org/10.1002/wfs2.1337).

[7]

H. Al-Khateeb, G. Epiphaniou, и H. Daly, «Blockchain for Modern Digital Forensics: The Chain-of-Custody as a Distributed Ledger», 2019. doi: [10.1007/978-3-030-11289-9\_7](https://doi.org/10.1007/978-3-030-11289-9_7).

[8]

M. Rafique и M. N. A. Khan, «Exploring Static and Live Digital Forensics: Methods, Practices and Tools», т. 4, вып. 10, 2013.

[9]

N. Marangos, P. Rizomiliotis, и L. Mitrou, «Digital forensics in the Cloud Computing Era», в *2012 IEEE Globecom Workshops*, Anaheim, CA, USA: IEEE, дек. 2012, сс. 775–780. doi: [10.1109/GLOCOMW.2012.6477673](https://doi.org/10.1109/GLOCOMW.2012.6477673).

[10]

J. T. Ami-Nart и P. A. H. Williams, «Digital forensics and the legal system: A dilemma of our times», *6th Australian Digital Forensics Conference*, т. Edith Cowan University, с. December 3rd 2008., 2006, doi: [10.4225/75/57B268CE40CB6](https://doi.org/10.4225/75/57B268CE40CB6).

[11]

D. J. Ryan и G. Shpantzer, «Legal Aspects of Digital Forensics».

[12]

A. Mitrakas и D. Zaitch, «Digital Forensics and the Chain of Custody to Counter Cybercrime».