Самат Ракимгалиевич Байгереев* – доктор PhD, ассоциированный профессор Международной школы инженерии ВКТУ им. Д. Серикбаева, г. Усть-Каменогорск; e-mail: sbaigereyev@edu.ektu.kz. ORCID: https://orcid.org/0000-0002-7773-5457.

Георгий Александрович Гурьянов – к.т.н., профессор Международной школы инженерии ВКТУ им. Д. Серикбаева, г. Усть-Каменогорск; e-mail: gguryanov@mail.ru. ORCID: https://orcid.org/0000-0003-3657-3735.

Received 04.02.2025
Revised 05.03.2025
Accepted 06.03.2025

https://doi.org/10.53360/2788-7995-2025-1(17)-11

МРНТИ: 81.93.29.

А.Р. Шалгынбаева
Евразийский национальный университет имени Л.Н. Гумилёва
010000, Республика Казахстан,г. Астана, Пушкина 11.
*e-mail: kaminariari16@gmail.com

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ИНСТРУМЕНТОВ КРИМИНАЛИСТИКИ: ENCASE И FTK IMAGER

Аннотация: *Дисковая форензика является важной областью информационной безопасности, направленной на исследование цифровых носителей с целью выявления, восстановления и анализа данных, имеющих значение в контексте расследований. В данной работе проводится исследование функциональности и производительности современных инструментов для анализа дисковой форензики. Основной акцент сделан на сравнении возможностей таких программ, как EnCase и FTK Imager, применяемых в данной сфере.*

В процессе исследования выполнен обзор существующих методов и технологий, лежащих в основе работы форензических инструментов, включая поиск удалённых файлов, восстановление файловых систем, анализ метаданных и выявление артефактов, указывающих на следы активности пользователей. Помимо функциональных возможностей, проводится анализ производительности программного обеспечения, включая скорость обработки данных, объем поддерживаемых форматов файлов и эффективность работы с большими объёмами информации.

Особое внимание уделено критериям оценки качества инструментов, таких как точность восстановления данных, пользовательский интерфейс и поддержка автоматизации задач.

Результаты исследования могут быть полезны для профессионалов в области кибербезопасности, судебной экспертизы и ИТ-администрирования, а также для студентов и исследователей, изучающих цифровую криминалистику. Работа направлена на расширение понимания возможностей и ограничений современных инструментов для анализа дисков, что способствует выбору оптимальных решений для конкретных задач.

Ключевые слова: *дисковая форензика, анализ данных, инструменты для криминалистики, восстановление файлов, цифровая криминалистика, информационная безопасность.*

Введение

В эпоху цифровых технологий и массовой цифровизации возникает необходимость защиты информации от кибератак, утечек данных и несанкционированного доступа. Сложность и количество киберпреступлений с каждым годом увеличиваются, заставляя специалистов искать новые методы и инструменты для расследования и предотвращения инцидентов. Важнейшим направлением цифровой криминалистики является дисковая форензика – процесс анализа цифровых носителей с целью восстановления и извлечения данных, имеющих значение для расследования преступлений.

Согласно отчету Herbert Smith Freehills, увеличение объема данных и множества источников требует тщательной подготовки и правильного выбора данных для сбора и анализа, с целью обеспечить успешное расследование. Эти слова подчёркивают важность развития новых подходов и технологий в области цифровой криминалистики.

В корпоративной среде утечки данных наносят компаниям значительные убытки, как финансовые, так и репутационные. Компании полагаются на дисковую форензику, чтобы

исследовать, откуда произошла утечка и кто мог быть к ней причастен. Например, инструменты форензики могут восстановить удаленные файлы, историю посещенных сайтов, следы использования USB-накопителей и другую информацию, что позволяет идентифицировать несанкционированный доступ к конфиденциальным данным.

Дисковая форензика также активно используется в расследованиях финансовых преступлений, где целью является выявление доказательств незаконной деятельности, таких как подделка финансовой отчетности, мошенничество с кредитными картами или схемы отмывания денег. Например, инструменты форензики могут извлекать информацию о финансовых транзакциях, которые были намеренно удалены или спрятаны в системе, помогая следственным органам установить связь между подозреваемой и преступной деятельностью. Мошенничество продолжает расти, и в 2022 году оно стало одной из ведущих причин киберинцидентов.

Кибератаки становятся всё более изощренными, и их расследование требует эффективных инструментов, способных извлекать следы атак на физическом уровне накопителей. Также после кибератаки необходим анализ цифровых носителей, который позволяет восстановить логи и файлы, поврежденные или скрытые вредоносным ПО. Дисковая форензика является неотъемлемой частью в области информационной безопасности, так как способствует идентификации файлов, используемые для несанкционированного доступа или передачи данных, что в свою очередь помогает отслеживать источники атак и предотвращать их повторение.

Методы исследования

Исследование функциональности и производительности инструментов для дисковой форензики основывалось на сочетании теоретических и практических подходов. На первом этапе был проведен анализ литературы и технической документации, что позволило определить наиболее эффективный инструмент, между EnCase и FTK Imager. Использовались научные публикации из специализированных журналов (Digital Investigation, Forensic Science International) и официальные руководства пользователей. Это позволило изучить их функциональные возможности, такие как поддержка различных файловых систем, восстановление данных, анализ метаданных и артефактов активности пользователей.

Для сравнения применялись разнообразные тестовые сценарии. Один из них включал восстановление удалённых файлов, где инструменты тестировались на наборе данных с удалёнными текстовыми документами, изображениями и видеофайлами. Другой сценарий предполагал анализ метаданных, при котором проверялись возможности извлечения временных меток, авторов и другой сопутствующей информации из файлов. Ещё одним важным аспектом стала обработка больших объёмов данных, где сравнивалась скорость обработки цифровых хранилищ объёмом до 1 ТБ.

Метрики оценки производительности включали скорость обработки данных, выраженную во времени, затраченном на выполнение сценариев. Также оценивалась точность восстановления данных, измеряемая в процентах от общего числа успешно восстановленных файлов. Удобство интерфейса анализировалось на основе обратной связи от пользователей, собранной в ходе анкетирования.

На основе результатов тестирования был проведен сравнительный анализ инструментов по следующим критериям: функциональность (спектр возможностей анализа и поддержки форматов), производительность (скорость работы и эффективность обработки больших объемов данных), удобство использования (интуитивность интерфейса, наличие автоматизации) и соотношение цена-качество (сравнение коммерческих лицензий и бесплатных решений).

Финальным этапом стало обобщение результатов и формирование практических рекомендаций для специалистов. Эти рекомендации учитывают специфические потребности различных групп пользователей: профессиональных судебных экспертов, корпоративных аудиторов и студентов. Применение комплексного подхода позволило обеспечить объективную оценку исследуемых инструментов, выявить их сильные и слабые стороны и предложить оптимальные решения для практического применения.

Обзор литературы

Применение дисковой форензики в корпоративной среде

Утечки данных являются одной из главных угроз для компаний. Восстановление удаленных файлов, анализ истории использования USB-устройств и посещенных веб-сайтов позволяет не только выявить источник утечки, но и идентифицировать лиц, причастных к инциденту. Например, EnCase предоставляет функции для углубленного анализа данных, включая восстановление доказательств, работающих даже в зашифрованных средах. FTK, в свою очередь, выделяется скоростью работы и простотой интерфейса, что делает его удобным инструментом для анализа больших массивов данных.

Согласно данным IBM, средняя стоимость утечки данных в 2024 году составила $4.88 миллиона, что подчеркивает важность быстрого и точного анализа для минимизации последствий инцидентов.

Расследование финансовых преступлений

Цифровая криминалистика играет важную роль в расследованиях финансовых преступлений, таких как подделка отчетности, мошенничество с кредитными картами и схемы отмывания денег. Инструменты, такие как EnCase и FTK, предоставляют возможности для анализа финансовых транзакций, включая восстановление удаленных или зашифрованных данных. В частности, EnCase позволяет обнаруживать сложные схемы махинаций благодаря расширенным функциям индексации и хэш-анализа.

Мошенничество остается одной из ведущих причин киберинцидентов. Инструменты форензики помогают установить причинно-следственные связи, что особенно важно для юридических расследований.

Кибератаки и их анализ

Современные кибератаки становятся всё более изощренными, требуя от инструментов форензики способности анализировать следы атак на физическом уровне. FTK предоставляет функции быстрого анализа логов и поврежденных файлов, что особенно полезно для расследования инцидентов, связанных с вредоносным ПО. EnCase, в свою очередь, обладает мощным функционалом для анализа цепочек сообщений и интернет-артефактов, что помогает определить источник атаки и предотвратить её повторение.

Согласно отчету Cybersecurity Ventures, киберпреступность будет наносить мировой экономике ущерб в размере $10.5 триллиона ежегодно к 2025 году. Это подчеркивает необходимость использования продвинутых технологий в цифровой криминалистике.

Обсуждение

В рамках цифровой криминалистики дисковая форензика играет важную роль в процессе анализа данных, предоставляя различные инструменты для решения различных задач. Однако выбор оптимального инструмента для выполнения конкретных задач зависит от множества факторов. В данном контексте рассмотрим два популярных инструмента – EnCase и FTK, с акцентом на их функциональные особенности, преимущества и недостатки.

Функциональность и возможности анализа

Диаграмма, представленная на Рисунке 1, отражает результаты сравнительного анализа функциональности двух широко используемых инструментов цифровой криминалистики — EnCase и FTK Imager. На основе литературных данных и технических спецификаций установлено, что EnCase демонстрирует значительно более широкий спектр функциональных возможностей, предлагая 18 ключевых функций против 12 у FTK Imager.

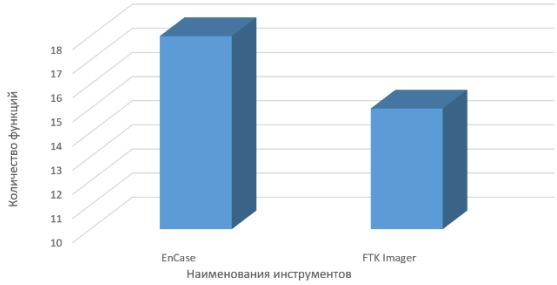

Рисунок 1 – Сравнительный анализ функциональности

Этот результат подтверждает превосходство EnCase в областях, требующих углубленного анализа данных, таких как обработка облачных данных, восстановление сложных артефактов и возможность кастомизации через встроенный язык EnScript.

Инструмент особенно эффективен для крупных организаций и корпоративных расследований, где важна глубокая аналитика и поддержка сложных форматов данных.

В свою очередь, FTK Imager концентрируется на скорости обработки и удобстве использования. Это делает его привлекательным решением для небольших организаций или специалистов, которые ценят простоту интерфейса и высокую производительность при анализе электронных писем и других базовых задач.

Таким образом, различия между инструментами оказывают значительное влияние на их практическое применение. EnCase подходит для пользователей, которым требуется глубокий анализ данных и возможность кастомизации, что делает его более предпочтительным для судебных расследований и корпоративных аудиторов. В то же время, FTK Imager удобен для специалистов, которым требуется быстрое восстановление данных и анализ без сложных конфигураций.

Скорость и производительность

На диаграмме, представленной на Рисунке 2, выполнен сравнительный анализ двух ключевых параметров инструментов цифровой криминалистики – скорости обработки данных и удобства использования. Оценка параметров осуществлялась по десятибалльной шкале, где значение 10 отражает максимальный уровень производительности и комфорта работы.

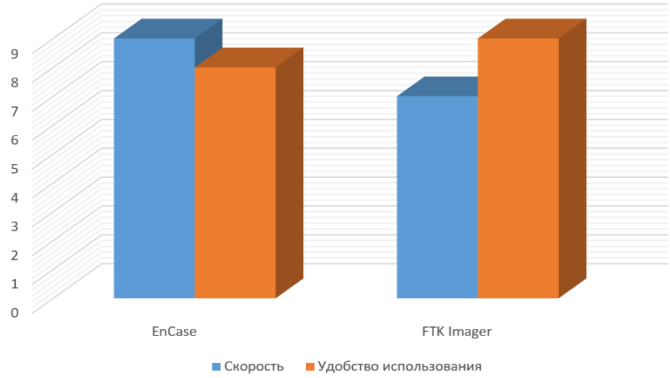

Рисунок 2 – Сравнительный анализ скорости и производительности

Для инструмента EnCase скоростные показатели были оценены на уровне 9 баллов, что соответствует высокой производительности при обработке данных. Однако незначительное снижение оценки удобства использования до 8 баллов свидетельствует о его сложной архитектуре и необходимости значительного времени для обучения пользователей, что делает его менее доступным для специалистов без соответствующего опыта.

Инструмент FTK Imager, напротив, демонстрирует обратную тенденцию: его удобство использования оценивается выше (9 баллов), что связано с интуитивно понятным интерфейсом и меньшими требованиями к обучению. Однако показатель скорости обработки данных (8 баллов) несколько ниже, что может быть связано с особенностями алгоритмов индексации, оптимизированных под обработку ограниченных массивов данных, таких как электронная почта и логи.

Эти различия позволяют сделать вывод, что EnCase подходит для анализа больших объемов данных, но требует времени на обучение, тогда как FTK Imager быстрее осваивается пользователями и подходит для оперативного анализа инцидентов. В результате, выбор инструмента зависит от срочности задачи и объема данных, с которым предстоит работать.

Поддержка платформ и расширяемость

EnCase отличается высокой степенью адаптации к различным операционным системам, включая Windows, Linux и Unix, что делает его универсальным решением для выполнения задач цифровой криминалистики. Инструмент поддерживает интеграцию с популярными облачными платформами, такими как Gmail и Google Drive, что значительно облегчает обработку удалённых и распределённых данных. Эти функции делают EnCase особенно полезным для крупных предприятий, работающих с большими массивами данных и сложными информационными структурами.

В отличие от EnCase, FTK ориентирован преимущественно на пользователей, работающих в Windows-среде. Несмотря на меньшую гибкость, инструмент остаётся

востребованным благодаря своему простому и понятному интерфейсу. Такие особенности делают его привлекательным выбором для малых организаций и специалистов, только начинающих изучение методов цифровой криминалистики.

Ограничения и вызовы

Несмотря на обширные функциональные возможности, оба инструмента имеют свои ограничения, которые могут влиять на их применение в различных сценариях:

EnCase требует значительных затрат времени и финансов для освоения, включая сложное обучение пользователей и высокую стоимость лицензий. Это может ограничивать его доступность для небольших организаций или индивидуальных специалистов.

FTK Imager, в свою очередь, характеризуется более простой эксплуатацией, но демонстрирует ограниченные возможности в поддержке сложных форматов данных и меньшую гибкость при настройке.

Оба инструмента также сталкиваются с системными вызовами, связанными с отсутствием стандартов данных. Недостаток унифицированных форматов усложняет обмен информацией между различными системами. Для повышения универсальности и эффективности данных инструментов требуется развитие многоязычной поддержки, что сделает их более пригодными для международных расследований и работы в глобальном контексте.

Следовательно, оба инструмента имеют свои слабые стороны, и их выбор должен основываться не только на функционале, но и на специфике работы организации. EnCase подходит для сложных корпоративных расследований, а FTK Imager является лучшим решением для оперативных анализов с минимальными затратами.

Применение в различных сценариях

Инструменты цифровой криминалистики используются в разных контекстах, включая судебные расследования, корпоративные проверки и реагирование на инциденты. Каждый из этих сценариев предъявляет свои требования к функциональности и возможностям EnCase и FTK Imager.

Судебные расследования.

EnCase является предпочтительным инструментом благодаря своей детализированной индексации, возможности создания надежных доказательных отчетов и строгому соответствию судебным стандартам. Поддержка EnScript позволяет автоматизировать сложные задачи, такие как выявление скрытых артефактов в зашифрованных файлах.

Корпоративные расследования.

Внутренние проверки на предмет утечек данных, несанкционированного доступа и экономических преступлений часто требуют быстрого анализа. FTK Imager обеспечивает оперативное сканирование устройств, анализ истории USB-устройств и восстановления удаленных данных, что делает его удобным инструментом для корпоративных аудиторов.

Реагирование на инциденты.

В условиях расследования кибератак критически важна скорость анализа данных. FTK Imager позволяет оперативно просматривать артефакты системы, журналы событий и возможные следы вредоносных программ. EnCase, в свою очередь, используется для более глубокого анализа инцидентов, когда необходимо выявить сложные техники уклонения злоумышленников и зашифрованные данные. Различия в функциональных возможностях данных инструментов подчёркивают их ориентированность на разные группы пользователей и соответствие специфическим сценариям применения в цифровой криминалистике:

Заключение

Сравнительный анализ показывает, что выбор подходящего инструмента должен основываться на специфике задач и масштабе расследования. EnCase является лидером в плане функциональности, предлагая интеграцию с облачными сервисами, поддержку сложных артефактов и гибкость настройки. В то же время, FTK Imager выигрывает за счёт своей скорости и простоты использования, что делает его идеальным выбором для случаев, требующих оперативного анализа или когда работа ведется с ограниченными ресурсами.

Ограничения обоих инструментов подчеркивают важность дальнейшего развития и адаптации этих решений к растущим требованиям современной цифровой криминалистики. Улучшение совместимости между системами и внедрение стандартов для обмена данными станут ключевыми направлениями их развития.

На основе проведенного анализа можно выделить несколько ключевых рекомендаций для специалистов, выбирающих инструмент цифровой криминалистики:

1) Если расследование требует глубокого анализа, работы с зашифрованными данными и сложной автоматизации, рекомендуется использовать EnCase. Этот инструмент подходит для судебных экспертов и крупных организаций, работающих с широким спектром данных.

2) Если основной приоритет – скорость и простота анализа, FTK Imager является оптимальным выбором. Он отлично подходит для корпоративных аудиторов, ИТ-специалистов и служб быстрого реагирования на инциденты.

3) В случаях, когда требуется комбинированный подход, возможно использование обоих инструментов. Например, FTK Imager может быть применен для первичного анализа и быстрого извлечения данных, а EnCase – для последующего детального изучения и построения отчетов.

Данный анализ подтверждает, что выбор между EnCase и FTK Imager зависит не только от функциональных возможностей, но и от специфики расследования. EnCase оказывается наиболее полезным в судебных и сложных корпоративных расследованиях, где критически важна детальная индексация данных и возможность глубокой автоматизации. В то же время FTK Imager находит свое применение в оперативных инцидентных расследованиях и корпоративных проверках, где ключевым фактором является скорость и удобство работы с доказательствами.

Таким образом, изучение производительности и функциональности инструментов анализа дисковой форензики показывает, что оба решения имеют свои сильные стороны и области для улучшения. В условиях постоянно растущих объемов данных и усложняющихся цифровых угроз их роль будет только возрастать, что делает актуальными вопросы повышения их эффективности и доступности для широкого круга пользователей.

Список литературы

1. Digital forensics in investigations and the growing data burden / S. Barrett et al // Herbert Smith Freehills, 2020. – URL: https://www.herbertsmithfreehills.com/insights/2020-07/digital-forensics-in-investigations-and-the-growing-data-burden.
2. IBM Security. Cost of a Data Breach Report 2024. – IBM, 2024. – URL: https://ibm.com/.
3. Association of Certified Fraud Examiners. Occupational Fraud 2022: A Report to the Nations. – ACFE, 2022. – URL: https://acfe.com/.
4. Cybersecurity Ventures. Cybercrime To Cost The World $10.5 Trillion Annually By 2025. – Cybersecurity Ventures, 2021. – URL: https://cybersecurityventures.com/.
5. Abdulkadir A. The Evaluation of EnCase and FTK Forensic Tools for Effective Evidence Extraction / A. Abdulkadir, A. Ahmad, B. Ja'afar // Global Scientific Journal. – 2021. – Vol. 9, Issue 3. URL: https://www.globalscientificjournal.com/.
6. EnCase Forensic. – OpenText, 2021. – URL: https://www.opentext.com/.
7. Forensic Toolkit (FTK). – AccessData, 2021. – URL: https://accessdata.com./
8. National Institute of Standards and Technology (NIST). Guide to Integrating Forensic Techniques into Incident Response. – NIST, 2020. – URL: https://www.nist.gov/.
9. Shinde P. Cybersecurity and Digital Forensics: A Survey on Tools and Techniques / P. Shinde, M. Gawali // International Journal of Computer Applications. – 2021. – Vol. 175, № 13. URL: https://www.ijcaonline.org/.
10. SANS Institute. Digital Forensics and Incident Response: Challenges and Tools. – SANS, 2021. – URL: https://www.sans.org/.

А.Р. Шалгынбаева

Еуразия ұлттық университеті Л.Н.Гумилев атындағы
010000, Қазақстан Республикасы, Астана қ., Пушкин көшесі, 11.
e-mail: kaminariari16@gmail.com

КРИМИНАЛИСТИКАЛЫҚ ҚҰРАЛДАРДЫ САЛЫСТЫРМАЛЫ ТАЛДАУ: ENCASE ЖӘНЕ FTK IMAGER

Дискілік форензика – бұл ақпараттық қауіпсіздік саласындағы маңызды бағыт болып табылады, оның мақсаты – цифрлық тасымалдаушыларды зерттеу арқылы тергеу тұрғысынан маңызы бар деректерді анықтау, қалпына келтіру және талдау. Бұл жұмыста дискілік форензикаға

арналған қазіргі заманғы құралдардың функционалдығы мен өнімділігін зерттеу жүргізілді. Негізгі назар осы салада қолданылатын EnCase және FTK Imager сияқты бағдарламалардың мүмкіндіктерін салыстыруға аударылады.

Зерттеу барысында форензикалық құралдардың жұмыс істеу негізінде жатқан әдістер мен технологияларға шолу жасалды, соның ішінде жойылған файлдарды іздеу, файлдық жүйелерді қалпына келтіру, метадеректерді талдау және пайдаланушылардың белсенділігінің іздерін көрсететін артефактілерді анықтау. Функционалдық мүмкіндіктерден басқа, бағдарламалық жасақтаманың деректерді өңдеу жылдамдығы, қолдау көрсетілетін файл пішімдерінің көлемі және үлкен көлемдегі ақпаратпен жұмыс істеу тиімділігі сияқты өнімділігі талданды.

Құралдардың сапасын бағалау критерийлеріне ерекше назар аударылды, мысалы, деректерді қалпына келтіру дәлдігі, пайдаланушы интерфейсі және тапсырмаларды автоматтандыруды қолдау.

Зерттеу нәтижелері киберқауіпсіздік, сот сараптамасы және IT-әкімшілендіру саласындағы мамандар үшін, сондай-ақ цифрлық криминалистика саласын зерттеп жүрген студенттер мен зерттеушілер үшін пайдалы болуы мүмкін. Жұмыс заманауи дискілік талдау құралдарының мүмкіндіктері мен шектеулерін түсінуді кеңейтуге бағытталған, бұл белгілі бір міндеттерді орындау үшін оңтайлы шешімдерді таңдауға ықпал етеді.

Түйін сөздер: *дискілік форензика, деректерді талдау, криминалистикалық құралдар, файлдарды қалпына келтіру, цифрлық криминалистика, ақпараттық қауіпсіздік.*

A.R. Shalgynbayeva
Eurasian National University named after L.N. Gumilyov,
010000, Republic of Kazakhstan, Astana, Pushkin St., 11
e-mail: kaminariari16@gmail.com

COMPARATIVE ANALYSIS OF FORENSIC TOOLS: ENCASE AND FTK IMAGER

Disk forensics is an essential area of information security aimed at examining digital storage devices to identify, recover, and analyze data relevant to investigations. This study focuses on the functionality and performance of modern tools for disk forensics analysis, with a primary emphasis on comparing the capabilities of programs such as EnCase and FTK Imager used in this field.

The research includes an overview of existing methods and technologies underlying forensic tools, including the search for deleted files, recovery of file systems, metadata analysis, and detection of artifacts indicating traces of user activity. In addition to functional capabilities, the study evaluates the performance of the software, including data processing speed, the range of supported file formats, and the efficiency of handling large volumes of information.

Special attention is paid to quality assessment criteria for the tools, such as data recovery accuracy, user interface, and support for task automation.

The results of the study may be valuable for professionals in cybersecurity, forensic investigation, and IT administration, as well as for students and researchers studying digital forensics. The work aims to enhance understanding of the capabilities and limitations of modern disk analysis tools, facilitating the selection of optimal solutions for specific tasks.

Key words: *disk forensics, data analysis, forensic tools, file recovery, digital forensics, information security.*

Сведения об авторах

Арина Руслановна Шалгынбаева – студент магистрант специальности «Системы информационной безопасности», Евразийский Национальный университет имени Л.Н. Гумилева, Республика Казахстан, г. Астана; e-mail: kaminariari16@gmail.com.

Автор туралы ақпарат

Арина Руслановна Шалгынбаева – «Ақпараттық қауіпсіздік жүйелері» мамандығы бойынша магистрант, Еуразия ұлттық университеті Л.Н. Гумилев атындағы, Қазақстан Республикасы, Астана қ.; e-mail: kaminariari16@gmail.com.

Information about the author

Arina Ruslanovna Shalgynbayeva – Master's student in the specialty «Information Security Systems», Eurasian National University named after L.N. Gumilyov, Republic of Kazakhstan, Astana; e-mail: kaminariari16@gmail.com.

Поступила в редакцию 11.03.2025
Поступила после доработки 13.03.2025
Принята к публикации 14.03.2025