Eurasian Journal of Applied Engineering and Technology (EJAET)

Научная статья https://doi.org/10.32523/3136-3385-2026-155-2-330-342

Разработка платформы киберполигона для начинающих специалистов по кибербезопасности

Т. Толеутай[1*], А. Ахметов[2], А. Жетписбаева[1], А. Куттыбек [1], А. Садвакасова[1]

[1] Astana IT University, Астана, Казахстан
[2] Satbayev University, Алматы, Казахстан

E mail: a.s.abdiraman@gmail.com, assemgul.sadvakasova@astanait.edu.kz, azhar.kuttybek@astanait.edu.kz, Aliya.Zhetpisbayeva@astanait.edu.kz, A.Zhenisbekkyzy@astanait.edu.kz

Аннотация. Стремительный рост киберпреступности, глобальный ущерб от которой к концу 2024 года достиг 9,5 трлн долларов США, а также активное использование злоумышленниками технологий искусственного интеллекта для кибершпионажа и проведения сложнообнаруживаемых атак обусловливают необходимость совершенствования подготовки специалистов по кибербезопасности. Несмотря на увеличение среднего значения глобального индекса кибербезопасности до 65,7 балла, уровень и сложность угроз продолжают расти, что требует внедрения практико-ориентированных и технологически гибких образовательных решений. В статье представлен систематический анализ существующих киберплатформ и выявлены их ключевые ограничения, включая отсутствие встроенных инструментов мониторинга, аналитики и персонализированной оценки прогресса обучающихся. В качестве решения разработана и реализована платформа киберполигона HackerPlace на базе Python Django, React.js, REST API и SQLite. Архитектура платформы построена по модульному принципу и включает клиентскую, серверную и аутентификационную подсистемы. Платформа поддерживает задания по веб-безопасности, OSINT, стеганографии, криптографии и реверс-инженерии, а также оснащена механизмами отслеживания времени и успешности выполнения задач. Апробация среди двух групп студентов показала повышение скорости решения задач на 32–58% и значительный рост общей результативности обучения.

Ключевые слова: Кибербезопасность, угрозы, платформа, киберполигон, CTF, Python, обучение на основе симуляции

Received 19.05.2025. Revised 20.05.2023. Accepted 24.11.2025. Available online 30.06.2026.

* the correspondence author

Введение

Сегодняшние реалии показывают, что ущерб от киберпреступности к концу 2024 года по всему миру составил 9,5 триллион долларов США. Масштабы атак увеличиваются с каждым годом, а хакеры все виртуознее используют инструменты по обходу системы защиты инфраструктуры и файрволов. С развитием искусственного интелекта злоумышленники начали использовать данный инструмент для проведения кибершпионажа и создания более сложных в обнаружении атак [1]. Согласно результатам проведенной статистики глобального индекса кибербезопасности в 2024 году средний показатель по всему миру составляет 65,7 балла, что на 27 процентов больше по сравнению с 2023 годом. Следовательно, возрастание киберугроз требует комплексного подхода при подготовке специалистов по защите и борьбе с киберпреступностью. Стоит отметить, что в данной области исследования набирают обороты и статистика с международной базы научных исследований Scopus показывает экспоненциальный рост исследований за последние пять лет. Результаты систематического литературного исследования представлены на рисунке 1.

В ходе исследования выявлен ряд платформ, которые предоставляют симуляционную среду в целях повышения квалификации специалистов по кибербезопасности. В работе [1] описываются основные ключевые моменты по платформе Cyberpolygon Site, который предназначен для подготовки специалистов по кибербезопасности. Аналогичные исследования проводились в работе [2], где также подготовлены задачи по симуляционным полигонам для защиты корпоративной сети. В работе [3] подробно описываются процесс разработки веб-приложения, который сочетает в себе как теорию, так и практические задания. Данного рода платформа помогает получить вводные теоретические знания в той или иной области симуляции атак.

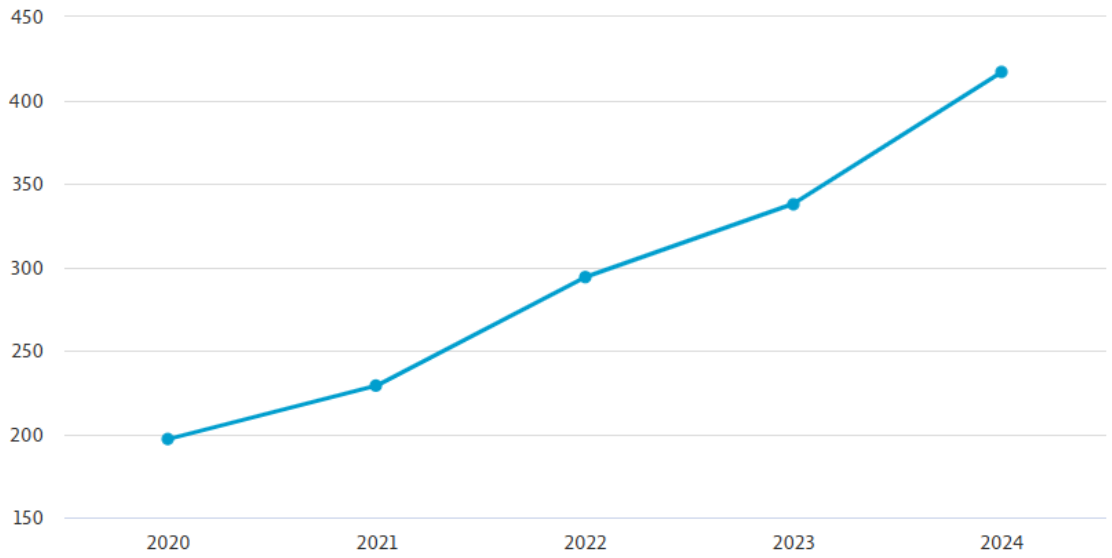

Рисунок 1. Статистика исследовании в области разработки киберполигонов за последние пять лет

Согласно исследованию в работе [4] рекомендуется применять метод геймификации в киберполигонах для образовательных учреждений. Статистика показала, что геймифицированные платформы значительно повышают вовлеченность и результатив-

ность студентов бакалавриата в области кибербезопасности.

Немаловажным аспектом является применение машинного обучения при автоматизации процессов в ходе защиты сложной инфраструктуры компании/предприятия. Следовательно, в работе [5] авторы подчеркивают, что машинное обучение является необходимым для подготовки кадров в части защиты от киберугроз. В работе [6] авторы проводят расширенный анализ первопроходцев по киберстартапам, что обусловливается положительными результатами с использованием инноваций в области кибербезопасности. Также исследования в [7-8] показали, что кибербезопасность также охватывает биологические системы защиты и технологию цифровых двойников по защите утечек данных и персональных данных пользователей. Кроме того, современные киберполигоны должны симмулировать реальные угрозы на различные информационные системы. Более того, применение киберполигона с интеграцией геймификации подтверждает увлеченность обучающихся, о чем говорят результаты статистических анализов, отраженные в работе [9-11].

Однако в ходе проведения литературного обзора выявлено, что все киберполигоны не предусматривают панель управления результатами обучающихся.

Методология

В процессе исследования применялись методы системного анализа, сравнительного анализа существующих платформ киберполигона, а также практической реализации и тестирования прототипа. На первом этапе проведён анализ зарубежных и отечественных решений, предназначенных для обучения специалистов по кибербезопасности (TryHackMe, RootMe, CyberPolygon и др.). На втором этапе осуществлёны дизайн и разработка платформы HackerPlace с использованием фреймворков Python Django и React.js, а также базы данных SQLite. На третьем этапе проведена апробация платформы среди студентов образовательной программы «Кибербезопасность» Astana IT University. Для оценки эффективности применялись методы экспериментального сравнения двух фокус-групп (A и B) с разным уровнем предварительной подготовки.

Полученные данные анализировались с использованием количественных показателей — среднего времени выполнения заданий, доли успешных решений, а также статистического сравнения результатов.

Выбор языка программирования для разработки платформы киберполигона. В ходе выбора языка программирования для разработки платформы киберполигона основное значение уделялось внятную интерфейсной части. Более того, серверная часть архитектуры киберполигона должна отражать логику системы.

Выбранные инструменты для разработки представлены в Таблице 1. В целях реализации авторизации обучающихся в систему киберполигона был применен фреймворк Django REST. То есть при авторизации веб-сайт отправляет запрос API для токенов в бэкенд. В свою очередь, бэкенд отправляет запрос в REST через просмотр. Сам токен генерируется в фреймворке REST. Данные пользователей собраны в базе данных через выделенные токены. Архитектура разработанной системы построена по модульному принципу и включает три основные подсистемы: клиентский интерфейс (Frontend), серверную часть (Backend) и компонент аутентификации, реализованные на основе REST-фреймворка. Взаимодействие между компонентами осуществляется посредством стандартизированных API-запросов [13]. Пользователь инициирует процессы регистрации или авторизации через клиентский интерфейс, который отправляет соответствующие запросы на Backend.

Серверная часть обрабатывает полученные данные, взаимодействует с хранилищем для сохранения или проверки учётной информации и далее направляет запрос к REST-фреймворку для генерации токена доступа. Сформированный токен передаётся обратно на клиентскую сторону, обеспечивая доступ к защищённым ресурсам. Система поддерживает механизм обновления токена: при его истечении Frontend инициирует запрос на продление, который проходит через Backend и обрабатывается соответствующим компонентом API. Такая схема позволяет обеспечить защищённое управление сессиями и контроль доступа к серверным ресурсам. Для наглядного представления взаимодействия компонентов в статью включена блок-схема общей архитектуры, иллюстрирующая полный цикл обработки запросов: от действий пользователя на клиентской стороне до генерации и обновления токена серверными подсистемами. На рисунке 2 представлена схема прохождения потока данных на платформе киберполигоне при регистрации пользователя.

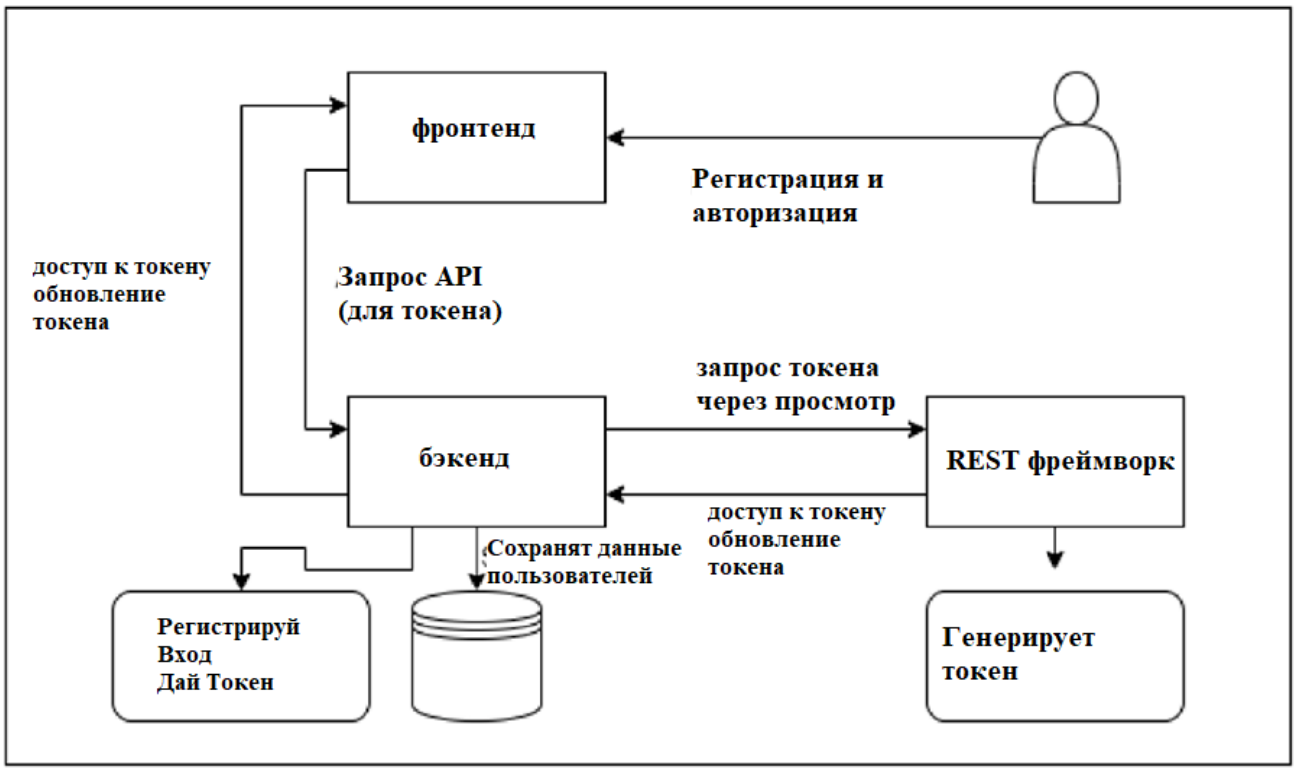

Рисунок 2. Схема регистрации и авторизации пользователя

Таймер расчета времени, потраченного на выполнение задания, в киберполигоне начинается, когда пользователь нажимает кнопку старта задания и кнопку стопа, когда завершает выполнение задания. На рисунке 3 представлена схема передачи данных внутри платформы. При разработке платформы HackerPlace были загружены различные сценарии задач, целью которых было получение опыта посредством тренировки в данной платформе. Данные задачи предусматривают получение практических навыков по темам: веб-безопасность, стеганография, OSINT, криптография, реверс-инженерия, SQL-инъекция. Каждая из данных тем разработана таким образом, чтобы предоставлять

сбалансированные теоретические и практические знания начинающим специалистам и выпускникам в области кибербезопасности [14].

Таблица 1. Выбранные инструменты для разработки платформы

Инструмент	Применение	Обоснование
Python	Бэкэнд	Простой и надёжный, с обширной библиотекой фреймворков для веб-разработки.
Django	Бэкэнд	Применяется данный фреймворк для веб-разработки на Python. Используется для управления результатами студентов.
React.js	Фронтэнд	Это библиотека в джаваскрипт для построения интерфейса пользователей.
REST	Веб API	Good for serialization and connecting backend with frontend
SQLlite	База данных	Lightweight, serverless and embedded SQL database engine. In combination with django gives high performance quality

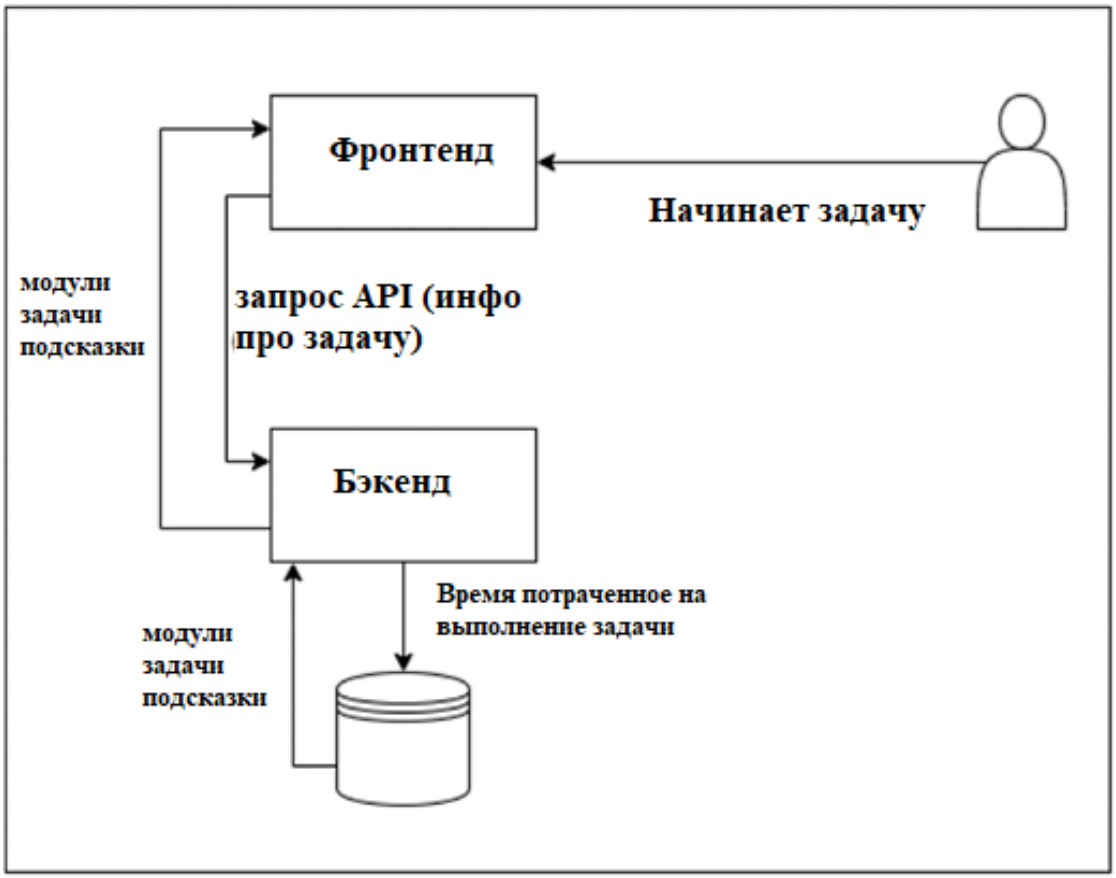

Рисунок 3. Схема выполнения задач

Админ-панель платформы HackerPlace

В данной секции статьи мы расскроем основные особенности и функционал кастомного решения по киберполигону отечественной разработки, который предназначен для улучшения контента при обучении специалистов кибербезопасности.

Данная платформа имеет интерактивный админ-панель, как представлено на рисунке 4.

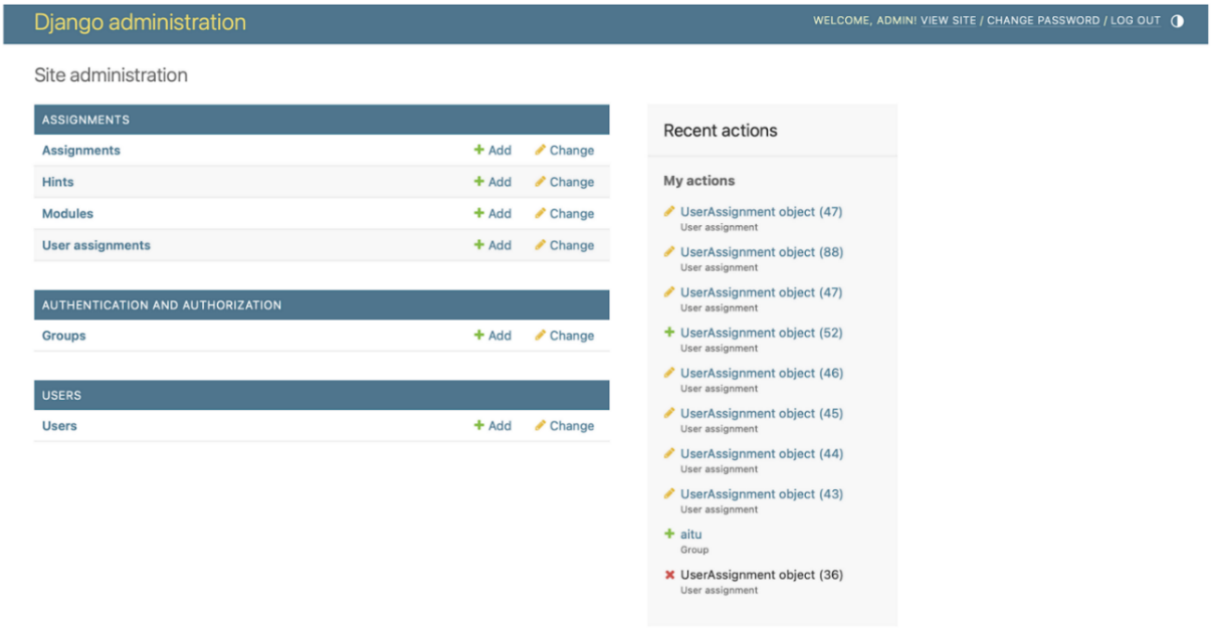

Рисунок 4. Админ-панель в Django

В части управления заданиями инструкторы могут создавать, редактировать, обновлять, добавлять дополнительные подсказки или же удалять устаревшие задачи. Также инструкторы могут добавлять теоретическое описание к заданиям и определять уровень сложности задания, как представлено на рисунке 5.

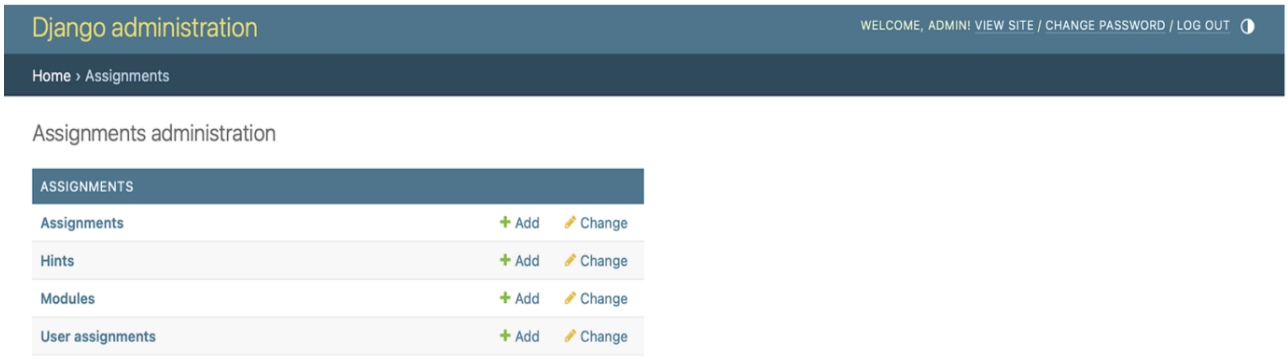

Рисунок 5. Панель управления задачами для обучающихся

На рисунке 6 представлен список задач, уже приготовленный для студентов, который включает в себя описание, подсказки и заголовки.

Стоит отметить, что пользователи с привилегиями администратора могут вносить изменения либо дополнять платформу, что очень удобно. В свою очередь, панель для обучающихся представлена на рисунке 7 и имеет очень удобный понятный интерфейс. Здесь по уровням можно увидеть различные модули, а под ними спрятаны задания и

подсказки по модулю.

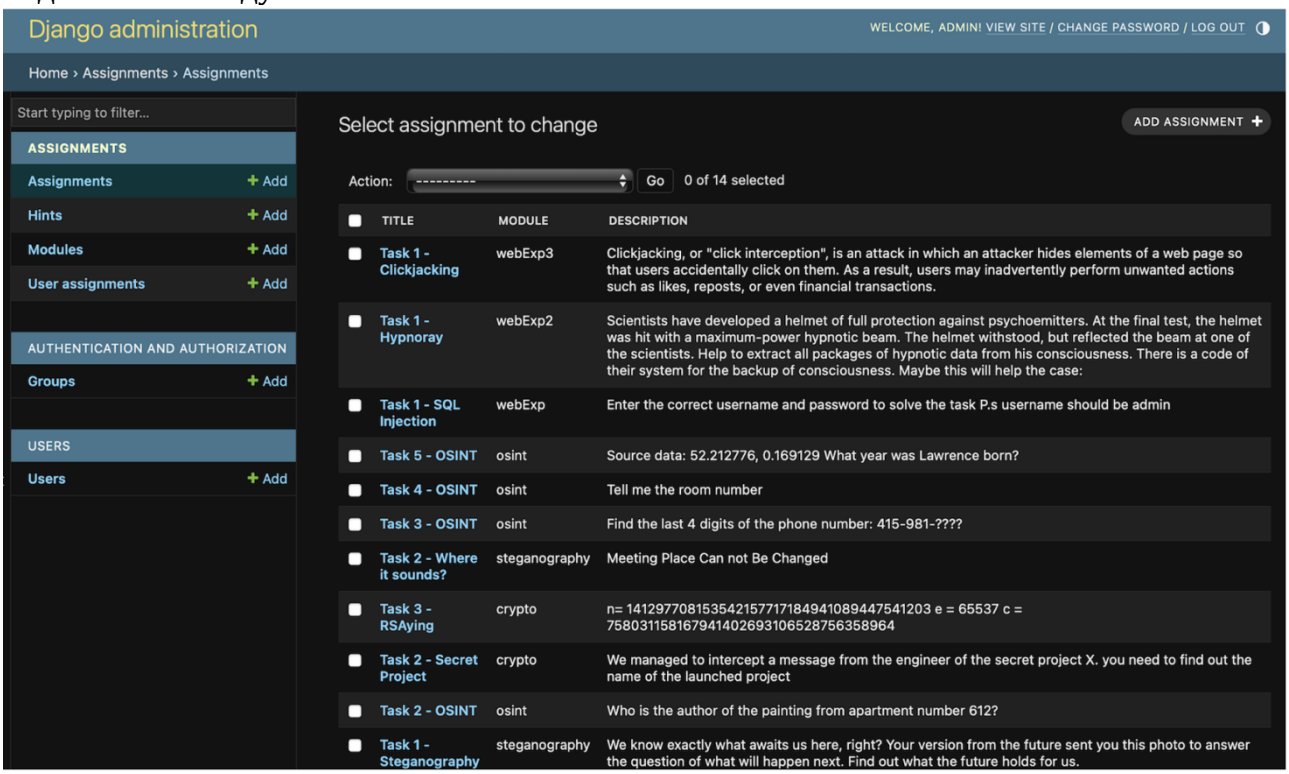

Рисунок 6 . Панель управления задачами

После нажатия на кнопку «старт» начинается отсчет времени по выполнению задания по выбранному направлению.

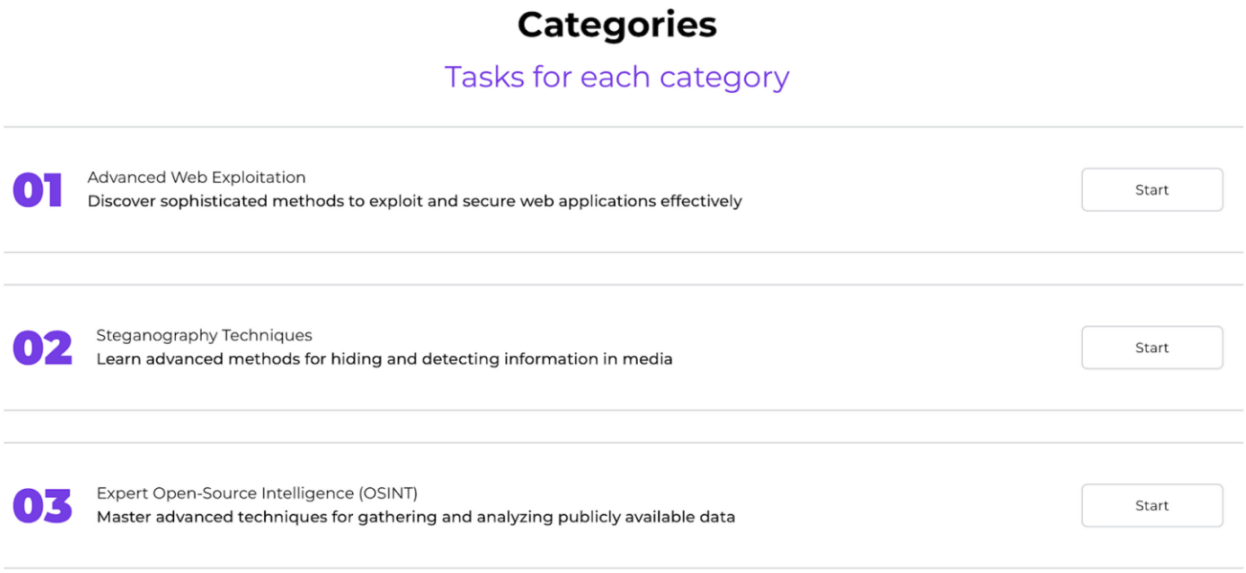

Рисунок 7. Категории заданий

На рисунке 8 представлен пример задания по категории OSINT. По данному направлению здесь загружено 5 задач, отсортированных по уровню сложности, есть окно добавления

ответа.

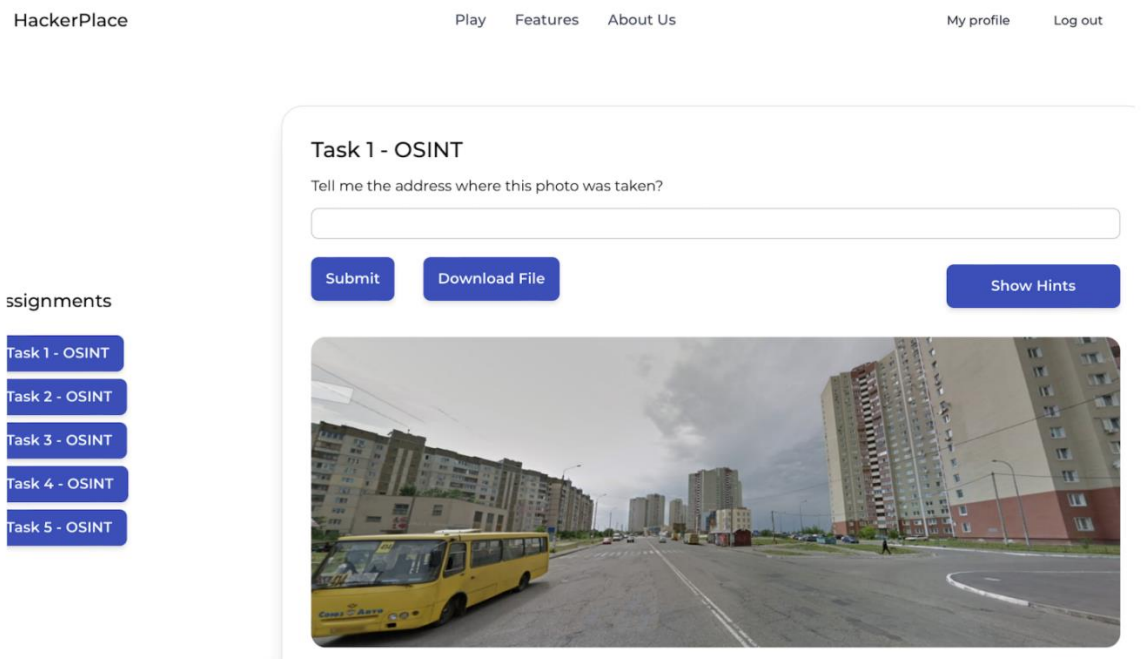

Рисунок 8. Страница задач OSINT

Также на данной платформе предусмотрена страница профиля пользователя, как и во многих платформах: TryHackMe, HackTheBox, RootMe.

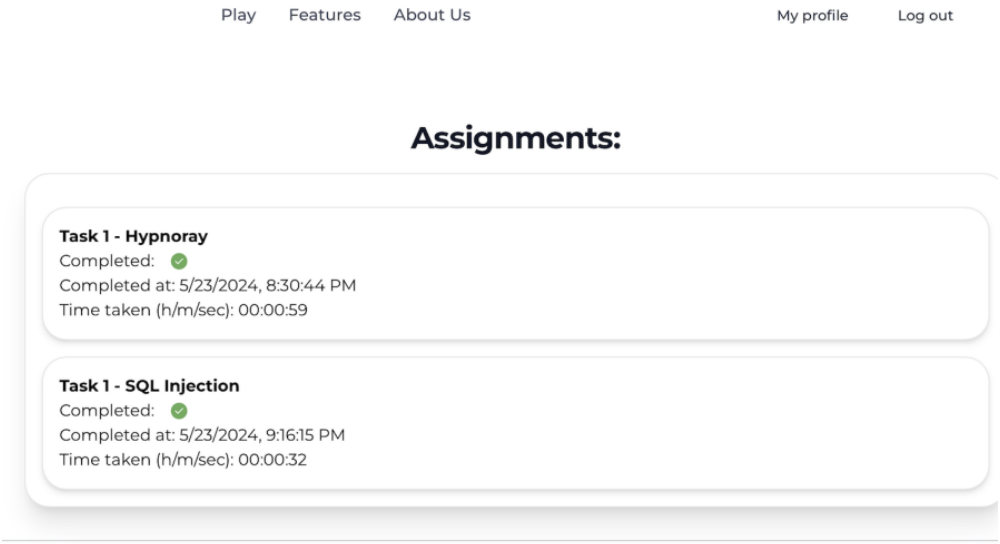

Рисунок 9. Механизм отслеживания времени выполнения заданий пользователями

На данной странице пользователь может видеть свой прогресс и выполненные задания. При правильном выполнении задания загорается зеленый цвет, что обозначает успешное прохождение задачи. Данная особенность позволяет оценивать успех и затруднения обучающего и фокусироваться на слабых сторонах [15]. На Рисунке 9 представлено время выполнения задания и сколько времени занимает в среднем это у пользователей платформы. Стоит отметить, что данная функциональная особенность платформы была

добавлена для проведения верификации посредством сравнения результатов студентов из университета А и университета В.

Аппробация платформы

Киберполигон Hacker Place был разработан и протестирован между двумя группами студентов для оценки эффективности использования такого подхода при обучении/повышении квалификации специалистов в области кибербезопасности. Студенты группы А регулярно использовали в обучении онлайн-платформы TryHackMe, RootMe, студенты группы В не использовали. Двум группам были даны задачи из данной платформы. В ходе исследования выявлено, что студенты группы А быстро решали задачи, нежели студенты группы В. В таблице 2 представлены результаты исследования.

Таблица 2. Среднее время выполнения задач по категориям

Катагория задания	Группа А (минуты)	Группа В (минуты)	Различие в процентах
Веб-безопасность	7.51	18.02	Группа А на 58.33% быстрее, чем группа В
Стегонаграфия	17.12	35.24	Группа А на 51.41% быстрее, чем группа В
OSINT	10.46	15.56	Группа А на 32.79% быстрее, чем группа В
Криптография	37.9	91.31	Группа А на 58.49% быстрее, чем группа В
Реверс-инженерия	41.03	64.78	Группа А на 36.65% быстрее, чем группа В

В таблице 3 представлены результаты участников по выполненным заданиям в разрезе по модулям киберполигона. Всего задач было 20, группа А успешно завершила 15 задач из 20 быстрее, чем группа В. Количество участников в обоих группах одинаковое.

Таблица 3. Рейтинг выполнения задач

Фокус-группа	Успешно выполненные задания	Общее количество участников	Рейтинг успешности в процентах
Группа А	15	20	75%
Группа В	5	20	25%

Следовательно, рейтинг успеха внутри группы А в три раза выше, чем в группе В. Данные результаты показывают эффективность применения киберполигонов в обучении и повышении квалификации.

Заключение

В данной статье был проведен анализ мировой практики в области обучения по кибербезопасности и борьбе с киберпреступностью. Актуальность создания такой платформы обосновывается растущим интересом к данной области. Различие разработанной нами платформы подчеркнуто ее гибкостью в части дополнения контентом. Также проведена апробация данной платформы посредством применения в

обучении в двух различных фокус- группах. В ходе апробации платформы в тестировании приняли участие 42 пользователя, включающие студентов направления «Кибербезопасность», а также начинающих специалистов, заинтересованных в практическом освоении методов этичного взлома. В рамках пилотного запуска было выполнено более 310 практических заданий, распределённых по четырём основным категориям: веб-безопасность, OSINT, стеганография и криптография. Среднее время выполнения задач и процент успешных попыток позволили провести сравнительный анализ подготовленности различных групп участников.Кроме того, по итогам тестирования был собран массив качественных отзывов. Более 78% пользователей отметили удобство интерфейса и интуитивную навигацию платформы, а 83% подтвердили, что выполнение практических упражнений помогло лучше понять принципы эксплуатации уязвимостей. Также пользователи предложили расширить каталог заданий и добавить дополнительные уровни сложности. Сводный анализ отзывов показал высокий уровень удовлетворённости и подтверждение практической ценности платформы на ранних этапах обучения в области кибербезопасности.

В заключение следует отметить, что разработанная платформа киберполигона представляет собой эффективный и научно обоснованный инструмент для подготовки начинающих специалистов по кибербезопасности. Её ключевая новизна заключается во внедрении адаптивного механизма оценки сложности задач и встроенной системы мониторинга прогресса обучающихся, что отсутствует в большинстве существующих решений. Предложенный подход обеспечивает объективную и воспроизводимую оценку компетенций, а архитектура платформы позволяет масштабировать систему за счёт расширения сценариев атак, подключения новых обучающих модулей и интеграции с образовательными и корпоративными тренинговыми средами. Полученные результаты апробации подтверждают практическую значимость платформы и её потенциал для дальнейших исследований в области симуляционного обучения и подготовки кадров по кибербезопасности.

Вклад авторов

Толкын Толеутай, Алибек Ахметов внесли существенный вклад в разработку концепции и дизайна исследования, а также в проектирование архитектуры платформы киберполигона HackerPlace. Авторы осуществили разработку клиентской и серверной частей системы, реализовали программную логику, включая механизмы аутентификации и мониторинга результатов, а также провели анализ и интерпретацию полученных технических результатов.

Жетписбаева Алия, Куттыбек Ажар внесли вклад в сбор, анализ и интерпретацию данных, выполнили систематический литературный обзор, провели сравнительный анализ существующих решений и сформировали теоретическое обоснование исследования. Помимо этого, авторы участвовали в подготовке и критическом пересмотре содержания статьи.

Садвакасова Асемгуль внесла вклад в написание текста статьи, сбор и статистическую обработку экспериментальных данных, их интерпретацию, а также организацию и проведение апробации разработанной платформы.

Список литературы

1. Miloslavskaya N., Tolstoy A. Cyber Polygon Site Project in the Framework of the MEPhI Network Security Intelligence Center // *Advances in Intelligent Systems and Computing.* — Springer Science and Business Media Deutschland GmbH, 2021. — Vol. 1310. — Pp. 295–308.
2. Galata L. P., Korniyenko B. Y., Yudin A. K. Research of the Simulation Polygon for the Protection of Critical Information Resources // *ITS.* — 2017. — November. — Pp. 23–31.
3. Fenton D., Traylor T., Hokanson G., Straub J. Integrating Cyber Range Technologies and Certification Programs to Improve Cybersecurity Training Programs // *The Challenges of the Digital Transformation in Education: Proceedings of the 21st International Conference on Interactive Collaborative Learning (ICL2018)-Volume 2.* — Springer International Publishing, 2019. — Pp. 632–643.
4. Jelo M., Helebrandt P. Gamification of Cyber Ranges in Cybersecurity Education // *2022 20th International Conference on Emerging eLearning Technologies and Applications (ICETA).* — IEEE, 2022. — October. — Pp. 280–285.
5. Apruzzese G., Laskov P., Montes de Oca E. et al. The Role of Machine Learning in Cybersecurity // *Digital Threats: Research and Practice.* — 2023. — Vol. 4, no. 1. — Pp. 1–38.
6. Lee D., Kim Y. First-Mover Advantages and Intentional Knowledge Spillover Effects on Cybersecurity Start-Ups' Financial and Innovation Performance: Incentive for Revealing Innovations in High-Tech Emerging Industry // *Asian Journal of Technology Innovation.* — 2022. — Pp. 1–19.
7. Schrom E., Kinzig A., Forrest S. et al. Challenges in Cybersecurity: Lessons from Biological Defense Systems // *Mathematical Biosciences.* — 2023. — P. 109024.
8. D. Lee, D. Kim, C. Lee, M. K. Ahn and W. Lee, "ICSTASY: An Integrated Cybersecurity Training System for Military Personnel," in IEEE Access, vol. 10, pp. 62232-62246, 2022, doi: 10.1109/ACCESS.2022.3182383
9. D. Qiu, M. Liu, R. Zhang, T. Luo, A. Griffo and X. Zhang, "Cyber-Physical Real-Time Digital Simulation for Cybersecurity Analysis in Microgrids," in *IEEE Transactions on Industrial Cyber-Physical Systems*, vol. 3, pp. 429-441, 2025, doi: 10.1109/TICPS.2025.3569640
10. Hart S. A Pedagogical Design Model to Create Serious Games for Cyber Security: Ph.D. thesis // *University of Southampton.* — 2022.
11. K. Fotiadou, T. -H. Velivassaki, A. Voulkidis, K. Railis, P. Trakadas and T. Zahariadis, "Incidents Information Sharing Platform for Distributed Attack Detection," in *IEEE Open Journal of the Communications Society*, vol. 1, pp. 593-
12. Yamin, M. M., Katt, B., Gkioulos, V. Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. Computers & Security, 2020. DOI: 10.1016/j.cose.2019.101636
13. Katsantonis, M. N., Manikas, A., Mavridis, I., Gritzalis, D. Cyber range design framework for cyber security education and training. International Journal of Information Security, 2023. DOI: 10.1007/s10207-023-00680-4
14. Glas, M., Vielberth, M., Pernul, G. Train as you Fight: Evaluating Authentic Cybersecurity Training in Cyber Ranges. Proceedings of CHI '23 (ACM), 2023. DOI: 10.1145/3544548.3581046
15. Jelo, M., Helebrandt, P.Gamification of cyber ranges in cybersecurity education. IEEE ICETA 2022, 2022. DOI: 10.1109/ICETA57911.2022.9974714

T. Toleutai[1*], A. Akhmetov[2], A. Zhetpisbayeva[1], A. Kuttybek [1], A. Sadvakasova[1]

[1] Astana IT University, Astana, Kazakhstan
[2] Satbayev University, Almaty, Kazakhstan

Development of a cyber range platform for cybersecurity beginners

Abstract. The rapid growth of cybercrime, with global damages reaching USD 9.5 trillion by the end of 2024, as well as the active use of artificial intelligence technologies by malicious actors for cyber espionage and hard-to-detect attacks, necessitate the improvement of cybersecurity specialist training. Despite the increase in the average Global Cybersecurity Index score to 65.7 points, the scale and complexity of threats continue to rise, requiring the implementation of practice-oriented and technologically flexible educational solutions. The article presents a systematic analysis of existing cyber platforms and identifies their limitations, including the lack of built-in tools for monitoring and analyzing learners' progress. As a solution, the HackerPlace cyber range platform was developed and implemented using Python Django, React.js, REST API, and SQLite. The system architecture follows a modular principle and includes client-side, server-side, and authentication subsystems. The platform supports tasks in web security, OSINT, steganography, cryptography, and reverse engineering, with mechanisms for tracking task completion time and success rates. Testing among two student groups demonstrated a 32–58% increase in task-solving speed and improved performance outcomes.

Keywords. Cybersecurity, threats, cyber range platform, CTF, python, simulation-based learning.

References

1. Miloslavskaya N., Tolstoy A. Cyber Polygon Site Project in the Framework of the MEPhI Network Security Intelligence Center // *Advances in Intelligent Systems and Computing.* - Springer Science and Business Media Deutschland GmbH, 2021. - Vol. 1310. -Pp. 295–308.
2. Galata L. P., Korniyenko B. Y., Yudin A. K. Research of the Simulation Polygon for the Protection of Critical Information Resources // *ITS.* - 2017. - November. - Pp. 23–31.
3. Fenton D., Traylor T., Hokanson G., Straub J. Integrating Cyber Range Technologies and Certification Programs to Improve Cybersecurity Training Programs // *The Challenges of the Digital Transformation in Education: Proceedings of the 21st International Conference on Interactive Collaborative Learning (ICL2018)-Volume 2.* - Springer International Publishing, 2019. - Pp. 632–643.
4. Jelo M., Helebrandt P. Gamification of Cyber Ranges in Cybersecurity Education // *2022 20th International Conference on Emerging eLearning Technologies and Applications (ICETA).* - IEEE, 2022. - October. - Pp. 280–285.
5. Apruzzese G., Laskov P., Montes de Oca E. et al. The Role of Machine Learning in Cybersecurity // *Digital Threats: Research and Practice.* - 2023. - Vol. 4, no. 1. -Pp. 1–38.
6. Lee D., Kim Y. First-Mover Advantages and Intentional Knowledge Spillover Effects on Cybersecurity Start-Ups' Financial and Innovation Performance: Incentive for Revealing Innovations in High-Tech Emerging Industry // *Asian Journal of Technology Innovation.* - 2022. - Pp. 1–19.
7. Schrom E., Kinzig A., Forrest S. et al. Challenges in Cybersecurity: Lessons from Biological Defense Systems // *Mathematical Biosciences.* - 2023. - P. 109024.

8. D. Lee, D. Kim, C. Lee, M. K. Ahn and W. Lee, "ICSTASY: An Integrated Cybersecurity Training System for Military Personnel," in IEEE Access, vol. 10, pp. 62232-62246, 2022, doi: 10.1109/ACCESS.2022.3182383
9. D. Qiu, M. Liu, R. Zhang, T. Luo, A. Griffo and X. Zhang, "Cyber-Physical Real-Time Digital Simulation for Cybersecurity Analysis in Microgrids," in *IEEE Transactions on Industrial Cyber-Physical Systems*, vol. 3, pp. 429-441, 2025, doi: 10.1109/TICPS.2025.3569640
10. Hart S. A Pedagogical Design Model to Create Serious Games for Cyber Security: Ph.D. thesis // *University of Southampton.* - 2022.
11. K. Fotiadou, T. -H. Velivassaki, A. Voulkidis, K. Railis, P. Trakadas and T. Zahariadis, "Incidents Information Sharing Platform for Distributed Attack Detection," in *IEEE Open Journal of the Communications Society*, vol. 1, pp. 593-
12. Yamin, M. M., Katt, B., Gkioulos, V. Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. Computers & Security, 2020. DOI: 10.1016/j.cose.2019.101636
13. Katsantonis, M. N., Manikas, A., Mavridis, I., Gritzalis, D. Cyber range design framework for cyber security education and training. International Journal of Information Security, 2023. DOI: 10.1007/s10207-023-00680-4
14. Glas, M., Vielberth, M., Pernul, G. Train as you Fight: Evaluating Authentic Cybersecurity Training in Cyber Ranges. Proceedings of CHI '23 (ACM), 2023. DOI: 10.1145/3544548.3581046
15. Jelo, M., Helebrandt, P.Gamification of cyber ranges in cybersecurity education. IEEE ICETA 2022, 2022. DOI: 10.1109/ICETA57911.2022.9974714

Сведения об авторах:

Толеутай Т. – автор для корреспонденции, магистрант, Astana IT University, Астана, Казахстан, пр. Мангилик ел 55/11, 010000
Ахметов А. – магистр, Satbayev University, Алматы, Казахстан.
Жетписбаева А. – магистр, сеньор лектор Школы Инженерии, Astana IT University, Астана, Казахстан.
Куттыбек А. – магистр, сеньор лектор Школы Кибербезопасности, Astana IT University, Астана, Казахстан
Садвакасова А. – магистр, сеньор лектор Школы Инженерии, Astana IT University, Астана, Казахстан

Toleutay T. – Corresponding author, Master's student, Astana IT University, Astana, Kazakhstan, 55/11 Mangilik El Ave., 010000
Akhmetov A. – Master's degree holder, Satbayev University, Almaty, Kazakhstan.
Zhetpisbaeva A. – Master's degree holder, Senior Lecturer at the School of Engineering, Astana IT University, Astana, Kazakhstan
Kuttybek A. – M.Sc., Senior Lecturer, School of Cybersecurity, Astana IT University, Astana, Kazakhstan
Sadvakasova A. – M.Sc., Senior Lecturer, School of Engineering, Astana IT University, Astana, Kazakhstan