ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ» КЕАҚ

Студенттер мен жас ғалымдардың
«ǴYLYM JÁNE BILIM - 2024»
XIX Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XIX Международной научной конференции
студентов и молодых ученых
«ǴYLYM JÁNE BILIM - 2024»

PROCEEDINGS
of the XIX International Scientific Conference
for students and young scholars
«ǴYLYM JÁNE BILIM - 2024»

2024
Астана

УДК 001
ББК 72
G99

«ǴYLYM JÁNE BILIM – 2024» студенттер мен жас ғалымдардың XIX Халықаралық ғылыми конференциясы = XIX Международная научная конференция студентов и молодых ученых «ǴYLYM JÁNE BILIM – 2024» = The XIX International Scientific Conference for students and young scholars «ǴYLYM JÁNE BILIM – 2024». – Астана: – 7478 б. - қазақша, орысша, ағылшынша.

ISBN 978-601-7697-07-5

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов имолодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001
ББК 72
G99

ISBN 978-601-7697-07-5

Преимущества использования Kali Linux через WSL для анализа флэш-накопителей очевидны и играют ключевую роль в обеспечении безопасности данных. Во-первых, этот подход гарантирует изоляцию среды анализа, что снижает риск заражения основной операционной системы в случае обнаружения вредоносных элементов на флэш-накопителе. Во-вторых, установка и настройка Kali Linux через WSL просты и доступны даже для неопытных пользователей. Благодаря этому, широкий круг пользователей может воспользоваться мощными инструментами, такими как Sleuth Kit, который значительно упрощает создание образов флэш-накопителей и анализ удаленных данных.

Применение методики использования Kali Linux через WSL в анализе флэш-накопителей предоставляет пользователям возможность эффективно выявлять потенциальные угрозы безопасности и принимать соответствующие меры для защиты данных. Этот подход не только обеспечивает безопасность и конфиденциальность информации, но и повышает уверенность пользователей в целостности и надежности их данных.

Необходимо отметить, что создание образа флэш-накопителя с помощью утилиты dd играет ключевую роль в процессе анализа. Создание образа позволяет сохранить целостность оригинальных данных, обеспечивая более точный и надежный анализ. Таким образом, использование Kali Linux через WSL открывает новые возможности для безопасного анализа флэш-накопителей и обеспечения защиты данных в цифровой среде с использованием Windows.

Список использованных источников

1. Oh J., Lee S., Hwang H. Forensic recovery of file system metadata for digital forensic investigation //IEEE Access. – 2022. – Т. 10. – С. 111591-111606.

2. Easttom C. Digital Forensics, Investigation, and Response. – Jones & Bartlett Learning, 2021.

3. Nikkel B. Practical Linux Forensics: A Guide for Digital Investigators. – no starch Press, 2021.

4. https://github.com/dorssel/usbipd-win/ - Windows software for sharing locally connected USB devices to other machines, including Hyper-V guests and WSL 2.

5. https://gitlab.com/alelec/wsl-usb-gui - WSL USB Manager to manage connecting USB devices from Windows to the WSL linux environment.

УДК 004.056.5

БОРЬБА С АКАДЕМИЧЕСКОЙ НЕЧЕСТНОСТЬЮ: ВНЕДРЕНИЕ ДВУХФАКТОРНОЙ АУТЕНТИФИКАЦИИ В СИСТЕМЫ УПРАВЛЕНИЯ ОБУЧЕНИЕМ ДЛЯ ПРЕДОТВРАЩЕНИЯ ФАЛЬСИФИКАЦИИ ДАННЫХ

Данияров Олжас Адылканович
olzhas.danayarov@mail.ru
Евразийский национальный университет имени Л. Н. Гумилёва
Научный руководитель старший преподаватель Аймичева Г.И.

Академическая нечестность, включая практику "buddy punching" и представление чужих работ, становится все более распространенной и серьезной проблемой в образовательной среде. Это явление подрывает целостность систем оценки, а также влияет на принципы справедливости и меритократии, лежащие в основе академического сообщества. В данном контексте внедрение метода двухфакторной аутентификации (2FA), основанного на использовании QR-кодов и одноразовых паролей (OTP), в системы управления обучением (LMS) представляет собой важный шаг в борьбе с академической нечестностью. Использование 2FA для входа в систему значительно усложняет возможность злоупотребления системой и представления чужих действий как своих собственных. Этот

метод обеспечивает дополнительный уровень безопасности и идентификации пользователей, что делает более сложным подделку или представление недостоверной информации. Помимо этого, внедрение 2FA способствует установлению четких цифровых следов действий пользователей, что повышает прозрачность и надежность процессов обучения и оценки.

Использование систем управления обучением с открытым исходным кодом (LMS), таких как Moodle, в учебных заведениях порождает проблемы безопасности и академической недобросовестности среди студентов. В этом случае лучшим способом избежать этого является использование двухфакторной аутентификации с помощью одноразового пароля (OTP) и кода быстрого реагирования (QR), который будет распространяться по различным каналам, так как при таком методе уменьшается потеря данных (злоумышленник не сможет получить второй фактор без пользователя). Также было отмечено, что в предыдущих исследованиях не рассматривался вопрос о том, что должен делать пользователь в ситуации, когда нет телефона. В данном исследовании эта проблема будет рассмотрена более подробно.

Цель исследования: Повышение безопасности систем управления обучением с открытым исходным кодом (LMS), таких как Moodle, в образовательных учреждениях.

В ходе исследования автор пытается ответить на следующий исследовательский вопрос: Как использование одноразовых паролей (OTP) и QR-кодов для электронной аутентификации влияет на уровень безопасности систем управления обучением (LMS), таких как Moodle?

Двухфакторная аутентификация для систем управления курсами (Moodle)

Исследователи предложили улучшить процесс шифрования и дешифрования ключей для обеспечения конфиденциальности данных. Однако данный метод остается сложным и требует много времени и усилий [1]. Другие авторы предложили систему, которая создает одноразовый пароль, встроенный в QR-код, с использованием общего секретного ключа для клиента и сервера [2]. Эта система требует аутентификации пользователей для доступа к системам, демонстрируя их авторизацию. Такой метод аутентификации по QR-коду и OTP обеспечивает высокий уровень безопасности и сохраняет конфиденциальность и надежность данных, поскольку для доступа необходимы два фактора: что-то, что пользователь знает, и что-то, что у него есть.

В различных исследованиях изучалась эффективность 2FA в Moodle, и некоторые из них показали, что она значительно снижает количество успешных попыток входа в систему злоумышленниками и повышает общую безопасность за счет снижения риска несанкционированного доступа и утечки данных [3, 4]. Несмотря на преимущества 2FA, его внедрение в Moodle сопряжено с такими проблемами, как принятие пользователями и техническая сложность реализации, особенно для небольших учебных заведений [5]. Для преодоления этих проблем были определены лучшие практики, такие как предоставление пользователям четких и кратких инструкций, предложение нескольких вариантов 2FA для учета различных предпочтений пользователей и возможностей устройств, а также проведение регулярных кампаний по обучению и повышению осведомленности для повышения уровня принятия пользователями. Если с точки зрения безопасности аутентификации проблема решаема, то возникает вопрос об удобстве входа в платформу для пользователей. В исследовании, проведенном в 2019 году, было опрошено 4 275 студентов, преподавателей и сотрудников Бригам-Янгского университета с целью выяснить отношение пользователей к двухфакторной аутентификации (2FA) один год после ее внедрения в университете [6]. Результаты опроса показали, что большинство участников почувствовали себя более защищенными с 2FA и считали его простым в использовании. Участники, ранее испытавшие нарушение безопасности, склонны рассматривать 2FA положительно, в то время как те, кто не сталкивался с нарушением безопасности, склонны видеть в нем негативные стороны. Авторы исследования пришли к выводу, что этот метод аутентификации для студентов и преподавателей не только более безопасен, но и более удобен в использовании.

Анализ данных опроса

Результаты опроса свидетельствуют о том, что более 83% преподавателей не испытали хакерские атаки на свои учетные записи Moodle. Однако, учитывая, что 14.3% респондентов подтвердили наличие подобного опыта, следует признать, что проблема безопасности данных в системах управления обучением, таких как Moodle, не является чем-то абстрактным или маловероятным (рис. 1). Это подчеркивает необходимость внедрения дополнительных мер безопасности, таких как двухфакторная аутентификация, для защиты учетных записей преподавателей и предотвращения фальсификации данных. Отмечается, что хакерские атаки могут иметь серьезные последствия, включая потенциальное нарушение конфиденциальности информации и угрозу целостности данных. Таким образом, внедрение двухфакторной аутентификации представляется эффективным способом укрепления безопасности систем управления обучением и борьбы с академической нечестностью.

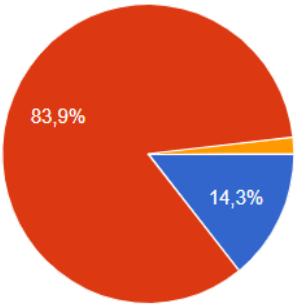


Рисунок 1. Сталкивались ли вы когда-нибудь с хакерской атакой на вашу учетную запись Moodle?

Результаты опроса показывают, что подавляющее большинство опрашиваемых (89.3%) считают, что внедрение двухфакторной аутентификации в системе Moodle поможет снизить академические проступки среди студентов (рис. 2). Это указывает на то, что существует высокий уровень уверенности в том, что такие дополнительные меры безопасности могут оказать положительное влияние на соблюдение академической честности. Однако, также отмечается, что небольшая часть респондентов (8.9%) не разделяют этой точки зрения. Это может быть связано с некоторыми опасениями или сомнениями относительно эффективности 2FA-аутентификации в борьбе с академической нечестностью. Тем не менее, общий тренд указывает на то, что внедрение таких мер безопасности в системы управления обучением, такие как Moodle, может способствовать снижению случаев академических проступков среди студентов.

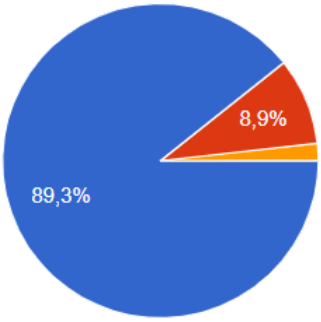


Рисунок 2. Считаете ли вы, что внедрение 2FA-аутентификации в системе Moodle поможет снизить академические проступки среди студентов?

Проектирование архитектуры системы

Судя по результатам опроса, преподаватели и студенты испытывают серьезные опасения по поводу безопасности учетных записей Moodle. Большинство респондентов считают, что добавление OTP повысит безопасность системы, при этом большинство респондентов указали, что такой способ защиты им будет удобен. Поэтому были разработаны сайт и мобильное приложение на базе Moodle LMS с 2FA, демонстрирующие безопасный метод авторизации пользователей.

Методология, использованная при разработке системы, включает систему двухфакторной аутентификации (2FA). Для этого пользователи должны предоставить комбинацию имени пользователя и пароля, одноразовый пароль (OTP) и выполнить сканирование QR-кода с помощью мобильного приложения (см. рис. 3). Кроме того, была реализована альтернативная версия двухфакторной аутентификации (2FA), требующая от пользователей предоставления имени пользователя и пароля. При отсутствии телефона для сканирования система предлагает ввести OTP-код. После точного ввода имени пользователя и пароля система переходит ко второму этапу, на котором OTP-код отправляется по электронной почте или номеру мобильного телефона (см. рис. 4). Примечательно, что код OTP является буквенно-цифровым, что повышает устойчивость к потенциальным словарным атакам.

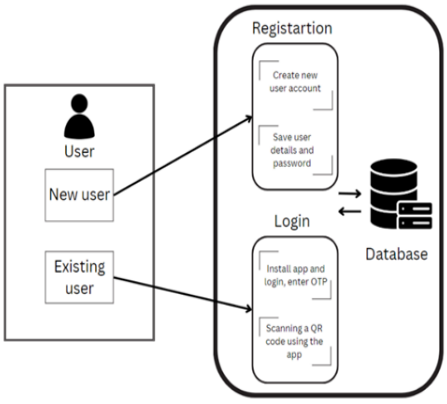


Рис. 3. Архитектура системы (QR-код)

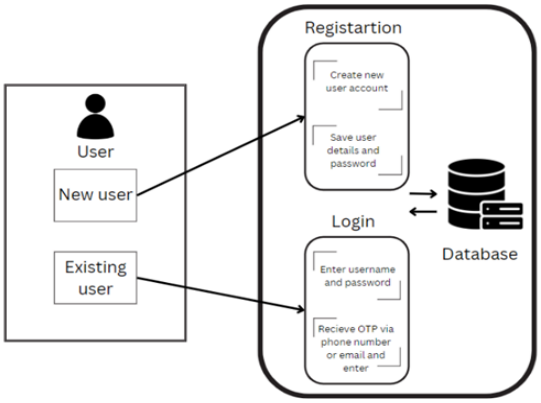


Рис. 4. Архитектура системы (OTP)

Основные инструменты, которые использовались для внедрения системы:

1. Серверная часть платформы сайта на Java (Java Spring Boot) => IntelliJ IDEA
2. Интерфейс платформы сайта на React JS => Визуальный код
3. Приложение на Flutter (язык Dart) => Android Studio
4. База данных => phpMyAdmin через MAMP

Два способа завершения процесса аутентификации для входа:

1) Когда пользователь нажмет кнопку входа, он будет перенаправлен на страницу OTP-аутентификации, которая представляет собой 2FA-аутентификацию путем ввода имени пользователя (баркода) и пароля при отсутствии телефона для сканирования (рис. 5). Затем пользователю необходимо выбрать способ получения OTP через номер телефона или электронную почту (рис. 6 (а), (б)) и ввести OTP-код в течение 2 минут (рис. 6 (в)).

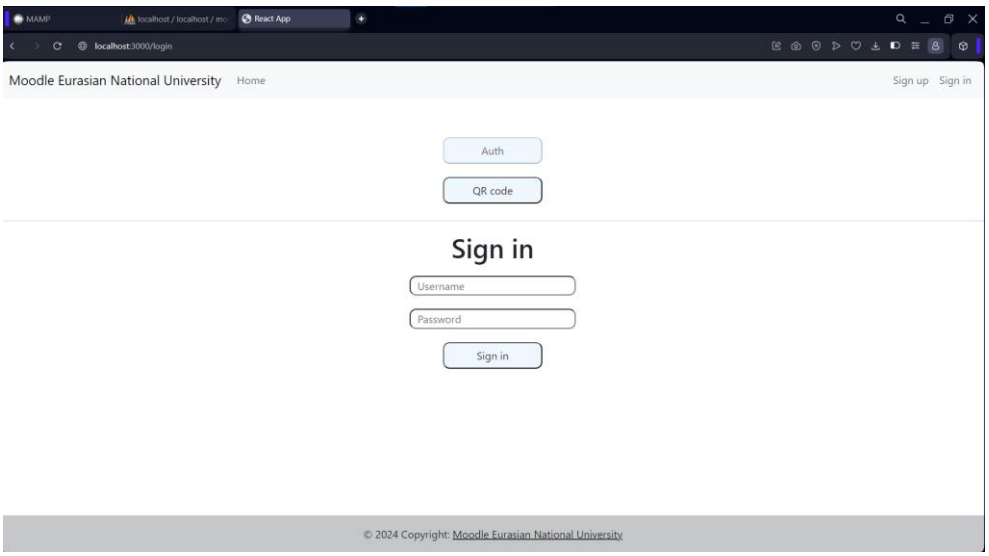
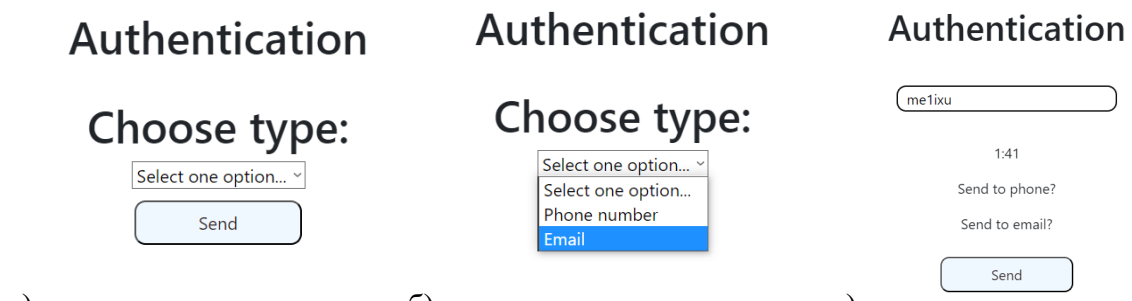


Рисунок 5. Страница входа (имя пользователя и пароль)



а) б) в)

Рисунок 6. Тип отправителя OTP

2) Пользователь также может пройти аутентификацию, нажав кнопку "QR-код" и отсканировав отобразившийся на сайте QR-код с помощью мобильного приложения системы (рис. 7). Но для этого пользователю необходимо ввести имя пользователя и пароль в приложении, после чего откроется окно для выбора способа получения OTP-кода. После успешного ввода OTP-кода пользователь будет перенаправлен в личный кабинет и сможет отсканировать его для входа на сайт, нажав на иконку QR-кода в мобильном приложении.

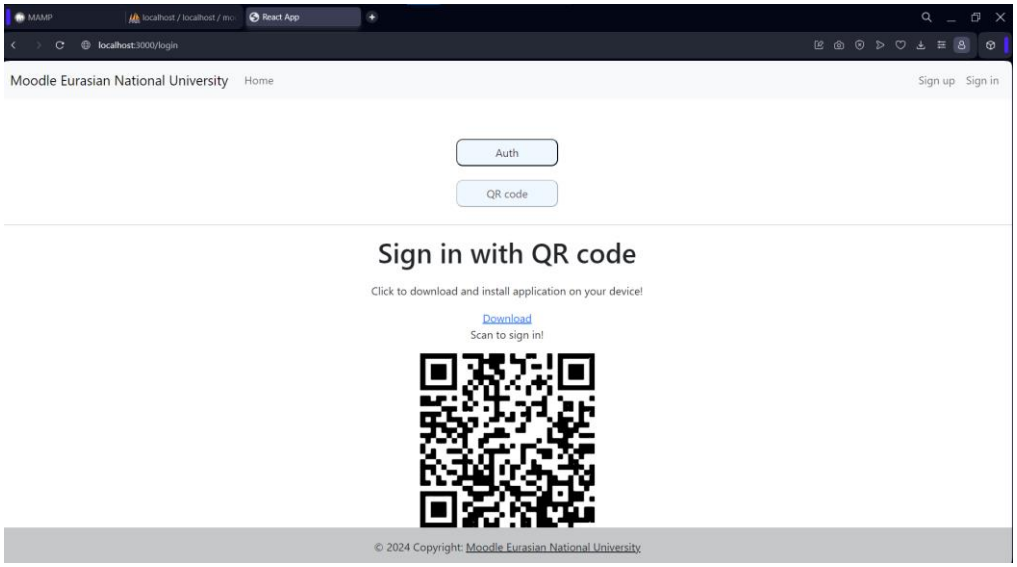


Рисунок 7. Страница аутентификации со сканированием QR-кода

В заключение хотелось отметить, что это исследование представляет собой многогранное исследование проблем в системах управления курсами, подчеркивая решающую роль безопасности, педагогики. Предлагаемая идея и решения подчеркивают необходимость комплексного, совместного и ориентированного на пользователя подхода для создания безопасной, поддерживающей и этически обоснованной академической среды. Ориентируясь в постоянно меняющемся ландшафте образовательных технологий, эта работа направлена на то, чтобы проложить путь к образовательным платформам, которые органично сочетают повышенные меры безопасности с глубокой приверженностью академической честности, что в конечном итоге способствует укреплению доверия и качества в высших учебных заведениях.

Список использованной литературы

1. Sheik, S. A., & Muniyandi, A. P. (2023). Secure authentication schemes in cloud computing with glimpse of artificial neural networks: A review. Cyber Security and Applications, 1, 100002. https://doi.org/10.1016/j.csa.2022.100002

2. Hassan, A., Shukur, Z., & Kamrul, M. (2020). An improved Time-Based One Time password authentication framework for electronic payments. International Journal of Advanced Computer Science and Applications, 11(11). https://doi.org/10.14569/ijacsa.2020.0111146

3. Mokalled, H., Catelli, R., Casola, V., Debertol, D., Meda, E., & Zunino, R. (2020). The guidelines to adopt an applicable SIEM solution. Journal of Information Security, 11(01), 46–70. https://doi.org/10.4236/jis.2020.111003

4. Arai, K. (2020). Adjacency effects of layered clouds by means of Monte Carlo ray tracing. International Journal of Advanced Computer Science and Applications, 11(1). https://doi.org/10.14569/ijacsa.2020.0110111

5. De Chérisey, É., Guilley, S., Rioul, O., & Jayasinghe, D. (2021). Information Theoretic Distinguishers for Timing Attacks with Partial Profiles: Solving the Empty Bin Issue. Journal of Information Security, 12(01), 1–33. https://doi.org/10.4236/jis.2021.121001

6. Dutson, J., Allen, D., Eggett, D. L., & Seamons, K. E. (2019). Don't Punish all of us: Measuring User Attitudes about Two-Factor Authentication. 2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), 119–128. https://doi.org/10.1109/eurospw.2019.00020

РАСШИФРОВКА ФАКТОРИЗАЦИИ - ВЫЗОВЫ КРИПТОГРАФИИ

Дурмагамбетов Асет[1], Дурмагамбетов Аслан[2]
[1]Преподаватель в ЕНУ имени Л.Н. Гумилёва
aset.durmagambetov@gmail.com
[2]Главный аналитик в Министерстве энергетики Республики Казахстан
tristesursi@gmail.com

Аннотация

В данной статье представлено описание нового метода решения проблемы факторизации, основанного на алгоритме градиентного спуска. Этот подход демонстрирует значительные улучшения в эффективности по сравнению с традиционными методами, предложенными в предыдущих исследованиях. В статье описывается новый метод решения проблемы факторизации на основе алгоритма градиентного спуска и демонстрируется переход от алгебраических методов к подходам, основанным на функциональном анализе. Предложенный подход не только повышает эффективность решения задачи, но также позволяет применять вычислительные алгоритмы функционального анализа, открывая новые возможности для исследований и оптимизации.

Ключевые слова: Дешифрование, проблема факторизации, алгоритм градиентного спуска, новый метод решения, переход от алгебраических методов к подходам, основанным на функциональном анализе.

Проблема факторизации, заключающаяся в поиске простых множителей составного числа, является одной из основополагающих задач в области криптографии и теории чисел. Эта проблема получила широкое распространение благодаря своему применению в алгоритме шифрования RSA, предложенном Rivest, Shamir и Adleman. Сложность задачи факторизации лежит в основе безопасности многих криптографических систем.

В последние годы было предложено несколько методов решения проблемы факторизации. К примеру, алгоритм квадратичного решета и метод поля чисел (1) демонстрируют высокую эффективность при работе с числами специфического размера. Однако, несмотря на их успех, они сталкиваются с серьезными вычислительными ограничениями при увеличении размера входных данных.

С развитием квантовых технологий возник новый интерес к алгоритмам факторизации, специально разработанным для квантовых компьютеров. Алгоритм Шора, предложенный в 1994 году, является одним из таких примеров, демонстрируя теоретическую возможность решения задачи факторизации за полиномиальное время на квантовом компьютере.