СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ

1. Иманалиева Ч.А., Суеркулова З.Т. Опыт внедрения элементов E-learning в учебный процесс. // Экономика. Управление. Образование. Международный научный журнал №2 (009). Б.- 2019. С.101-107

Румянцева А.С. методы оценки качества образовательной услуги «Инженерный класс» // Вестник науки №10 (43) том 3. С. 37 - 42. 2021 г. ISSN 2712-8849 // Электронный ресурс: https://www.вестник-науки.рф/article/4821

Malcolm McDonald. Web Security for Developers: Real Threats, Practical Defense. Illustrated Edition. ISBN-13: 978-1593279943, ISBN-10: 1593279949

The LMS Guidebook: Learning Management Systems Demystified - Steve Foreman. ISBN 978-1607283096.

Creating Learning Organizations Through Digital Transformation -(редакторы: Henrique S. Mamede & Arnaldo Santos). IGI Global, 2024. ISBN 9798369305584. books.google.com

The Digital Transformation Playbook: Rethink Your Business for the Digital Age - David L. Rogers. Columbia Business School Publishing, 2016. ISBN 978-0231175449. Columbia University Press

Digital Transformation in Higher Education: 7 Areas for Enhancing Digital Learning - Florence Martin & Kui Xie. 2022. EDUCAUSE Review

УДК 004.056.53.5

Муктарбеков Санат Муктарбекович
Сануриптик инновациялар академиясы, магистрант
Кыргыз Республикасы, Бишкек ш.
e-mail: kubanychbekm8888@gmail.com
Зимин Игорь Викторович
Сануриптик инновациялар академиясы
педагогика илимдеринин кандидаты, доцент,
Кыргыз Республикасы, Бишкек ш.
e-mail: igorzimin777@mail.ru

БИЛИМ БЕРҮҮ ВЕБ-ПЛАТФОРМАСЫНДА АР КАНДАЙ КООПСУЗДУК ТЕХНОЛОГИЯЛАРЫН ИНТЕГРАЦИЯЛОО ЖАНА ТЕСТИРЛӨӨ

Аннотация. Макала билим берүү веб-платформаларындагы маалыматтарды коргоо технологияларын интеграциялоо жана тестирлөө маселелери изилдөөгө арналат. Анда колдонуучулардын маалыматтарын иштетүү жана сактоо үчүн коопсуз чөйрөнү түзүүнүн негизги аспектилери, анын ичинде заманбап шифрлөө ыкмаларын, аутентификация жана авторизация системаларын колдонуу, ошондой эле платформаларды үзгүлтүксүз аудиттен өткөрүү баяндалат. Макалада платформаны иштеп чыгуу этаптары, коопсуздукту тестир-лөө жана интеграцияланган коргоо технологияларынын артыкчылыктары көрсөтүлүп, GDPR сыяктуу укуктук нормаларды сактоонун жана колдонуучулардын кызыгуусун арттыруу үчүн геймификация практикасын колдонуунун маанилүүлүгү белгиленет. Бул изилдөөнүн натыйжалары билим берүү платформаларын иштеп чыгуучуларга, администраторлорго жана сануриптик билим берүү стандарттарын түзүүчүлөргө пайдалуу.

Негизги сөздөр: билим берүү платформалары, маалыматтарды коргоо, шифрлөө, коопсуздукту тестирлөө, GDPR, геймификация, аутентификация, веб-иштелме.

Муктарбеков Санат Муктарбекович
Академия цифровых инноваций, магистрант
Кыргызская Республика, г. Бишкек
e-mail: kubanychbekm8888@gmail.com
Зимин Игорь Викторович
Академия цифровых инноваций
кандидат технических наук, доцент.
Кыргызская Республика, г. Бишкек
e-mail: igorzimin777@mail.ru

ИНТЕГРАЦИЯ И ТЕСТИРОВАНИЕ РАЗЛИЧНЫХ ТЕХНОЛОГИЙ ЗАЩИТЫ В ОБРАЗОВАТЕЛЬНОЙ ВЕБ-ПЛАТФОРМЕ

Аннотация. Статья посвящена исследованию интеграции и тестирования технологий защиты данных в образовательных веб-платформах, рассмотрению ключевых аспектов разработки безопасной среды для обработки и хранения пользовательских данных, включая применение современных методов шифрования, систем аутентификации и авторизации, а также регулярный аудит платформ. В статье освещены этапы разработки платформ, тестирования ее безопасности, а также преимущества использования интегрированных технологий защиты. Акцентируется внимание на важности соблюдения правовых норм, таких как GDPR, и применении практик геймификации для повышения вовлеченности пользователей. Материалы исследования могут быть полезны разработчикам, администраторам образовательных платформ и лицам, формирующим стандарты в сфере цифрового образования.

Ключевые слова: образовательные платформы, защита данных, шифрование, тестирование безопасности, GDPR, геймификация, аутентификация, веб-разработка.

Muktarbekov Sanat Muktarbekovich
Academy of Digital Innovations, Master's student
Kyrgyz Republic, Bishkek
e-mail: kubanychbekm8888@gmail.com
Zimin Igor Viktorovich
Academy of Digital Innovations,
Candidate of Technical Sciences, Associate Professor
Kyrgyz Republic, Bishkek
e-mail: igorzimin777@mail.ru

INTEGRATION AND TESTING OF DIFFERENT SECURITY TECHNOLOGIES IN AN EDUCATIONAL WEB PLATFORM

Annotation. The article is devoted to the study of integration and testing of data protection technologies in educational web platforms, consideration of key aspects of developing a secure environment for processing and storing user data, including the use of modern encryption methods, authentication and authorization systems, as well as regular auditing of platforms. The article highlights the stages of platform development, testing of its security, as well as the advantages of using integrated protection technologies. It emphasizes the importance of complying with legal regulations, such as GDPR, and applying gamification practices to increase user engagement. The research materials can be useful for developers, administrators of educational platforms and those who form standards in the sphere of digital education.

Keywords: educational platforms, data protection, encryption, security testing, GDPR, ramifications, authentication, web development.

Цифровизация образования требует от разработчиков создания веб-платформ, которые обеспечивают удобный доступ к материалам и могут гарантировать защиту пользовательских данных. Рост числа онлайн-курсов и сервисов ведет к увеличению объема информации, которую необходимо защищать от несанкционированного доступа, и это делает безопасность ключевым элементом функционирования образовательных веб-платформ.

В данной статье мы рассматриваем основные подходы к интеграции и тестированию технологий защиты данных образовательных веб-платформ, их роль в обеспечении безопасности пользователей и повышения доверия к онлайн образованию.

Образовательные площадки хранят и обрабатывают огромное количество данных пользователей, результаты тестирования и учебно-методические материалы. Эти данные подвергаются постоянным угрозам. Наиболее распространёнными из которых являются:

– кибератаки - SQL-инъекции, DDoS атаки, межсайтовые скриптовые XSS атаки;

– утечка данных - некорректная ошибки в настройке систем хранения данных и человеческий фактор;

– недостатки аутентификации - использование слабых паролей и отсутствие двухфакторной аутентификации;

– вредоносное ПО - загрузка зараженных файлы и фишинговые атаки.

Вышеперечисленные угрозы требуют внедрения самих технологий защиты и их постоянное тестирование.

Для реализации комплексной защиты данных мы предлагаем использовать следующие технологии:

– Шифрование - базовый метод защиты данных, который используется и вовремя передачи данных и при их хранении. В образовательных платформах применяются такие методы как HTTPS - защищенный протоколы передачи данных для предотвращения их перехвата злоумышленниками, и шифрование базы данных - алгоритмы AES-256 и RSA, применяемые для защиты хранимых данных. Например, внедрение SSL/TLS-сертификатов позволяет обеспечить защищенное соединение между клиентом и сервером, минимизируя риск утечки данных.

– Аутентификация и авторизация - двухфакторная аутентификация (2FA) и управление ролями. Например, на электронной платформе Moodle реализована ролевая модель доступа, в которой преподаватели имеют доступ к созданию курсов, а студенты – только к их прохождению.

– Защита от внешних атак – параметризованные запросы против SQL-инъекций, фильтрация вводимых данных и использование заголовков CSP (Content Security Policy) для предотвращения XSS и распределенные сети для защиты от DDoS-атак.

– Регулярный аудит и тестирование – постоянный мониторинг безопасности системы и пентесты, (penetration tests) помогающие выявлять и устранять слабые места в защите данных до того, как ими воспользуются злоумышленники.

Интеграция технологий защиты в образовательные платформы предполагает следующие этапы:

– анализ рисков - определение уязвимостей системы;

– выбор технологий - использование подходящих решений в зависимости от масштаба платформы;

– внедрение – настройка механизмов шифрования данных, брандмауэров, аутентификации, журналирования и резервного копирования;

– тестирование - проверка корректности работы защитных механизмов и устранение ошибок;

– мониторинг - постоянное отслеживание активности на платформе для выявления аномалий и обновление системы.

Интеграция технологии машинного обучения позволяет автоматизировать анализ данных, выявлять подозрительные активности и предсказывать появление новых угроз. Например, аномальное поведение пользователя (частая смена IP-адресов, множественные неудачные попытки входа) введет к его автоматической блокировке.

Для оценки устойчивости обучающей веб-платформы мы рекомендуем проводит регулярное тестирование ее защиты для выявления потенциальных угроз.

Виды тестирования:

– функциональное тестирование - проверка корректности работы механизмов защиты системы;

– нагрузочное тестирование – симуляция высоких нагрузок для определения устойчивости платформы при массовом использовании;

– пентесты - имитация внешних атак на систему для выявления слабых мест.

– тестирование пользовательского интерфейса - проверка удобства доступности элементов безопасности.

Автоматизированные инструменты для проверки функциональной безопасности системы:

1. OWASP ZAP (Zed Attack Proxy) - открытый инструмент для автоматического сканирования уязвимостей, который подходит для тестирования как небольших, так и крупных веб-приложений. В основном он используется для обнаружения SQL-инъекций и XSS.

2. Burp Suite – один из популярных инструментов для тестирования безопасности различных веб-приложений, позволящий проводить анализ трафика, тестировать уязвимости и настраивать специфические сценарии тестирования.

3. Metasploit - платформа для проведения пентестов и имитации кибератак, которая обычно используется для тестирования систем на устойчивость к реальным внешним угрозам.

4. Nessus - инструмент для анализа конфигураций и сканирования уязвимостей, формирующий детализированные отчеты о найденных проблемах и предлагающий пути их устранения.

Средства тестирования нагрузок:

1. Apache JMeter – симулирует высокую нагрузку на сервер и анализирует его производительность. Например, проверяет стабильность веб-платформы при одновременном входе большого количества пользоватлей.

2. Gatling - имитирует стресс-тесты на на веб-приложениях, при этом он отличается высокой скоростью и масштабируемостью.

Инструменты для анализа безопасности кода:

3. SonarQube – проводит статический анализ исходного кода, обнаруживает потенциальные уязвимости и помогает улучшать качество кода.

4. Checkmarx – анализирует безопасность приложений и предоставляет рекомендации по исправлению найденных уязвимостей.

Интеграция и тестирование технологий защиты являются ключевыми этапами при разработке образовательных веб-платформ. В совокупности с регулярным тестированием и мониторинга они обеспечивают безопасность данных пользователей, предотвращают кибератаки и повышают доверие к системе.

Разработка комплексных решений в области кибербезопасности способствует устойчивому развитию цифрового образования и формированию безопасной образовательной среды.

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ

1. Cybersecurity Management in Education Technologies: Risks and Countermeasures for Advancements in E-learning (ред. Ahmed A. Abd El-Latif, Yassine Maleh, Mohammed A. El-Affendi, Sadique Ahmad). CRC Press, 2024.

2. Grokking Web Application Security (Malcolm McDonald). O'Reilly, 2023–2024.

3. Secure Web Application Development: A Hands-On Guide with Python and Django (Matthew Baker). Apress, 2022.

4. Information Security in Education and Practice (Kalinka Kaloyanova, ред.). Cambridge Scholars Publishing, 2023.