УДК 371.321.1

ЦИФРОВОЕ ОБРАЗОВАНИЕ: ПРОБЛЕМЫ БЕЗОПАСНОСТИ И ЛУЧШИЕ ПРАКТИКИ

Холов Ш.Ё.

Таджикский технический университет имени академика М.С.Осими, Душанбе, Таджикистан, sh.kholov88@gmail.com

Аннотация. В результате этого исследования криптографический механизм становится методом наилучшей защиты конфиденциальности, аутентификации и аутентификации (ЦРУ) данных на электронных платформах. Однако недостаточно силен, чтобы смягчить кибербезопасность. По этой причине предполагается, что механизм шифрования не должен сочетаться с другими методами, такими как биометрическая аутентификация, межсетевые экраны, IDS, цифровые водяные знаки и модели процессов.

Ключевые слова. Цифровое образование, безопасность, проблемы, меры.

1. ВВЕДЕНИЕ

Цифровое обучение проводится уже в процессе обучения на нескольких уровнях. Однако быстрое развитие технологий и вспышек COVID-19 изменили образовательную среду на более интенсивное обучение. Таким образом, использование технологий на всех уровнях образования стало повсеместно. Например, платформа онлайн-обучения обеспечивает общедоступные бесплатные курсы; приложения для видеоконференций, предоставляющие студентам и преподавателям неограниченное время для видео, перевода и возможности совместного редактирования. Кроме того, школы сотрудничают с телевидением для трансляции образовательного контента на отдельных каналах [1]. Технология может обеспечить высокое качество и большую гибкость образовательный опыт без ограничений, принятый в традиционной образовательной среде, такой как строгий график или класс. Он может стать дополнительным аксессуаром для подключения, творческого и персонализированного обучения. Кроме того, корпорация также использует цифровое образование для обучения сотрудников. В сетевых образующих платформах предусмотрены различные меры для улучшения бизнеса, безопасности, соблюдения требований и технологии. Хотя технологии открывают некоторые возможности в сфере образования, они также создают риски в сфере разработки и развертывания. Манипулирование устройствами, утечка информации, сетевая атака и последующий эффект платформенных приложений – это угроза безопасности, обнаруженная при использовании технологий [2,3]. Еще одним аспектом, который следует считать барьером при использовании современных технологий, является отсутствие знаний в области образования в области информационной безопасности [4]. Таким образом, данное исследование сосредоточено на этих аспектах безопасности. Угрозы и предлагают решения, которые могут применяться учителями и учениками при использовании технологий для образовательных целей.

2. ПРОБЛЕМЫ БЕЗОПАСНОСТИ

2.1 Проблемы безопасности платформы

2.1.1 Moodle (Модульная объектно-ориентированная динамическая среда обучения)

Moodle – это система электронного обучения с открытым исходным кодом. Он использует язык PHP и базы данных MySQL, предлагая учителям и ученикам различные модули для создания уроков, заданий, викторин, документы и упражнения. Кроме того, это помогает учителям и учащимся общаться друг с другом через чат, опросы или семинары. Атака методом грубой силы представляет собой уязвимость безопасности, присутствующую в этом платформе. Эта атака угадывает пароли и имена пользователей, отправляя несколько запросов на веб-сервер с пустым полем cookie, чтобы сбросить счетчик неудачных входов в систему до нуля. Думать имя пользователя, многие имена пользователей поставляются со случайным паролем. Обычно, если ответ от сервер расширен, шансы угадать пользователя высоки. Атака перехвата сеанса. Эта атака захватывает контроль над сеансом пользователя при успешном получении или генерирование идентификатора сеанса аутентификации. Это связано с тем, что злоумышленник использует захваченные, грубые, или идентификаторы сеансов, полученные методом реверс-инжиниринга, чтобы взять под контроль сеанс веб-приложения легального пользователя, пока эта сессия все еще продолжается. Сеанс обрабатывается в Moodle с использованием двух файлов cookie: Moodle Тест сеанса и сеанса Moodle, который можно прервать, поскольку Moodle использует только SSL. Туннели в службе входа в систему и нескольких службах администрирования. Таким образом, HTTP-запросы в виде открытого текста, который может быть перехвачен и декодирован. Злоумышленник может использовать эти данные в своих HTTP-запрос для управления сеансом целевого пользователя. Аналогичным образом, несколько типов атак связаны с аутентификация, доступность, конфиденциальность и целостность данных в системе Moodle [5].

2.1.2 Масштабирование Zoom

Zoom – это платформа, которая помогает студентам и преподавателям общаться удаленно. Он дает множество преимуществ, таких как простота установки, дружественный интерфейс и бесплатное использование. Однако он сталкивается с несколькими угрозами безопасности, такими как масштабирование, сквозное шифрование, шпионаж за Mac, удаленное выполнение кода Windows, уязвимости Cisco Talos [6]. В 2021 году [7] сообщалось, что в цепочках атак с тремя ошибками использовалось удаленное выполнение кода (RCE) на машине жертвы. Другое исследование [8] выявило более

десяти типов проблем безопасности и конфиденциальности в Zoom. По данным [9], в Zoom было обнаружено множество дыр в безопасности, и две из них могут позволить хакерам читать и красть данные пользователей.

2.1.3 Blackboard

Blackboard – это комплексное цифровое образовательное пространство, позволяющее повысить персонализированное обучение пользователей в любое время и в любом месте. Он предлагает множество инструментов для поддержки учебной и преподавательской деятельности, таких как Blackboard Analytics, Центр оценок, оценка доски, аккредитация, взаимодействие с доской и многое другое. Тем не менее, он также уязвим для многих проблем безопасности, как и другие платформы. Например, в 2010 году было обнаружено 84 проблемы безопасности, связанные с платформой Blackboard. Примечательно, что команда LaQuSo сообщила о трех значимых типах атак в версии досок SP5, таких как подделка межсайтовых запросов, атаки с использованием межсайтовых сценариев и уязвимости авторизации [10].

2.1.4 Платформа edX

Эта платформа предоставляет высококачественный опыт обучения различным университетам, организациям и учреждениям. Он представляет пакет данных edX, который включает сбор данных об использовании курсов на страницах курса edX. Однако он представляет собой несколько уязвимостей для пользователей, таких как межсайтовый скриптинг (XSS), фишинг паролей, выполнение кода на стороне сервера и идентификация данных RDX.

– XSS: это одна из самых популярных проблем безопасности в Интернете. Это дает хакерам возможность внедрить на сайт клиентские скрипты. XSS-червь был разработан для внедрения каждого раздела, подраздела или модуля каждого курса и помещения его в модуль. Более того, этот червь может автоматически использовать вредоносные скрипты для заражения каждого юнита на трассе.

– Фишинг паролей. Фишинговые атаки более опасны для студентов, которые используют один и тот же пароль на разных сайтах, и хакеры могут получить доступ к учетным записям студентов на платформе edX.

– Идентификация данных RDX. RDX – это еще один способ обеспечения безопасности и функционального компромисса. Он может предоставить ценные инструменты для поиска показателей удержания студентов и факторов, которые поддерживают учащихся и эффективно используют ресурсы сайта. Это также повышает эффективность онлайн-образование. Однако он предоставляет сторонним исследователям большие наборы данных, что потенциально рискованно.

2.2 Внешние кибератаки

2.2.1 Вредоносные атаки

Компьютерные вирусы, вредоносные программы, трояны – это вредоносные программы, которые могут изменить или повредить операционную систему без разрешения пользователя, используя вложенные файлы в электронном письме или рекламных объявлениях. Когда студенты или преподаватели загружают ресурсы в электронную систему, можно легко одновременно загрузить вредоносные коды. Кроме того, студенты могут использовать свои собственные устройства для поиска информации, сотрудничества или общения с другими студентами для обучения в кампусе и за его пределами. Следовательно, контроллеру данных сложнее обеспечить безопасность сетевой системы от вирусов, троянов или вредоносных программ. Кроме того, студенты являются основными пользователями социальных сетей. Таким образом, это может создать подходящую среду для распространения вирусов, вредоносных программ и других вирусов через эти веб-сайты социальных сетей.

2.2.2 Атака доступности

Целью этой атаки является прерывание ресурсов подключения или ограничение пропускной способности электронных систем. Более того, он также пытается получить привилегированный доступ к информации или услугам на образовательной платформе. DoS-атаки или DDoS-атаки не являются новыми типами угроз. Однако их ущерб гораздо опаснее, чем в предыдущие годы. Объем DDoS-атак и их сложность резко возросли из-за снижения стоимости запуска этого типа атак. Поэтому сложно обнаружить и защитить системы от них. Согласно отчету «Лаборатории Касперского», в 2019 и 2020 годах в системах электронного обучения произошло значительное количество DoS-атак (Securelist, 2020). В 2020 году он увеличился на 550% по сравнению с аналогичным периодом 2019 года (январь). Zoom – самая популярная платформа, подвергшаяся атаке, а Moodle – вторая. При этом рекламное ПО, загрузчики и трояны встречались почти в 99% от общего числа зарегистрированных попытки заражения.

2.2.3 Атака на конфиденциальность

Эта атака в основном направлена не на изменение содержания данных, а на ограничение доступа к данным и их распространения. Эта атака имеет три основные категории: небезопасное криптографическое хранилище, небезопасная прямая ссылка на объект, утечка информации и неправильная обработка ошибок.

– Небезопасное криптографическое хранение: системы электронного обучения редко используют криптографические механизмы для защиты данных. Поэтому конфиденциальные данные можно хранить в хранилище или базе данных без шифрования.

– Небезопасная прямая ссылка на объект: электронная система использует ссылки на объекты (файлы, записи данных и первичные ключи) в веб-интерфейсах, но без использования каких-либо методов проверки авторизации.

– Утечка информации и неправильная обработка ошибок: конфиденциальная информация или данные могут быть непреднамеренно раскрыты через сообщения об ошибках.

2.2.4 Атаки на целостность

Существует множество типов уязвимостей электронного обучения от внешних атак, таких как вредоносные коды, такие как CSS или XSS, подделка межсайтовых запросов (CSRF), прямое внедрение кода SQL на веб-страницы, переполнение буфера, невозможность ограничения доступа по URL-адресу, Ошибки внедрения и вредоносное выполнение файлов.

– Подделка межсайтовых запросов (CSRF): опасная уязвимость, поскольку она может выполнить несанкционированное действие на платформе с законным доступом и согласием пользователя.

– Недостатки внедрения (InjecF): хакеры могут внедрить входные данные (SQL-запрос) на клиентской рабочей станции в приложение для чтения, изменения или выполнения конфиденциальных данных в базе данных.

– Выполнение вредоносного файла: вредоносные коды могут быть интегрированы во время функции загрузки, и система не сможет управлять производительностью загруженных файлов.

2.2.5 Атаки аутентификации

Такого рода атаки происходят, когда хакеры незаконно получают пароли пользователей и пытаются получить свободный доступ к материалам систем электронного обучения. Кроме того, когда происходит такая атака, хакерам легко получить возможность выполнить другие типы атак, например, атаки на доступность, конфиденциальность и целостность. Есть две основные категории: нарушение аутентификации и управления сеансами, а также атаки на небезопасную связь.

– Нарушение аутентификации и управления сеансами. Хакеры могут перехватить или украсть аутентифицированные сеансы легальных пользователей, включая активные сеансы, пароли и токены сеансов.

– Небезопасная связь. Во время передачи данных токены сеанса или конфиденциальная информация без использования механизма шифрования могут быть использованы злоумышленниками для доступа к незащищенным разговорам и получения учетных данных пользователя.

3. КОНТРМЕРЫ

В этом разделе описаны различные контрмеры по защите систем электронного обучения:

3.1 Криптография

Криптография – это метод, гарантирующий конфиденциальность данных и их неразглашение неавторизованным лицам (Файзиева и др., 2019) (Costinela-Luminita, 2011). Это процесс преобразования данных из источника в непонятный формат. Его можно использовать во многих электронных системах с различными средствами для обеспечения передачи данных в Интернете. Механизм криптографии использует множество математических алгоритмов, связанных с информационной безопасностью, для защиты данных, таких как конфиденциальность, целостность и аутентификация. Шифрование с симметричным ключом и шифрование с асимметричным ключом являются важнейшими типами методов шифрования.

3.2 Управление цифровыми правами

Законы, убеждения и практика определяют цифровые права. В виртуальном пространстве управление цифровыми правами (DRM) является важной стратегией, которую необходимо интегрировать, особенно в электронном обучении, чтобы уменьшить риски, связанные с активами, услугами и ресурсами электронного обучения (Эль-Софани и др., 2013. Он представляет собой приложение для электронного образования со стандартами и технологиями, поддерживающими совместное использование или повторное использование электронных учебных ресурсов.

3.3 Решение с распределенным межсетевым экраном

Распределенные межсетевые экраны включают в себя множество резидентных программных приложений безопасности для защиты сетей, пользователей и серверов организаций от неожиданного вторжения [11]. Однако существует значительная разница между персональным и распределенным межсетевым экраном. Последнее дает больше преимуществ, таких как централизованное управление, отчеты о журналировании и детализация контроля доступа. Эти функции можно использовать на предприятиях для взаимодействия с политиками безопасности внутри межсетевого экрана. Кроме того, брандмауэр предлагает различные преимущества, такие как защита сетей или системы от внутренних и внешних атак, уменьшая количество отдельных точек отказа, обеспечивая безопасность удаленные компьютеры конечных пользователей и защита хостов.

3.4 Биометрическая аутентификация

Для сохранения паролей в секрете используются традиционные методы аутентификации, такие как пароли, смарт-карты, цифровые подписи и цифровые сертификаты. Параллельно биометрическая аутентификация является новым методом повышения безопасности. Это также лучший выбор, помогающий пользователям избежать неправильного использования пароля при отправке заданий и документов, а также при загрузке материалов курса.

3.5 Цифровые водяные знаки

Цифровые водяные знаки – это новый метод, который позволяет пользователям размещать скрытые примечания об авторских правах, аудио, видео и изображения. Следовательно, несанкционированное использование в системах электронного обучения можно предотвратить с помощью цифровых водяных знаков. Существует два основных типа цифровых водяных знаков: видимые и невидимые. Первый использует встроенные алгоритмы, менее сложные вычисления и простое распознавание. Последнее затрудняет просмотр или распознавание водяных знаков зрителями или читателями.

3.6 Меры противодействия кибератакам

Из-за среды Интернета электронная система также подвергается кибератакам, как и Интернет. Таким образом, согласно, существует множество способов защитить электронное обучение от кибератак, например, использование безопасного протокола HTTPS, системы обнаружения инструкций, межсетевых экранов. и криптографические механизмы. Эти методы могут обеспечить целостность, доступность, аутентификацию и конфиденциальность цифровых систем от внешних атак. Более того, существует множество решений для защиты систем электронного обучения. Примечательно, что для Moodle вход в систему с использованием капчи и SSL является лучшим методом, позволяющим избежать атак методом перебора и защитить сеанс между веб-сервером и браузером. Кроме того, применение многофункциональной биометрической аутентификации для аутентификации учащихся на платформах электронного обучения, в

том числе по лицу, голосу, прикосновению, мыши и нажатию клавиши, является потенциальным, гибким и надежным решением для идентификации учащихся. Электронное обучение – это облачная среда. Он использует преимущества облака вычислительные технологии. Однако могут возникнуть некоторые проблемы безопасности, связанные с облачными вычислениями. Следовательно, для решения этих проблем безопасности могут использоваться различные механизмы, такие как информационная безопасность SMS, безопасность биометрической информации, информационная безопасность на основе токенов, список контроля доступа, информационная безопасность цифровых подписей, криптография и безопасная платформа электронного обучения на основе архитектуры SOA. Этот метод кардинально меняет образование, поскольку может помочь создать целостную систему управления образовательными достижениями.

4. ВЫВОДЫ

Образованию пришлось быстро адаптироваться к ситуации с пандемией. Традиционные методы обучения были заменены цифровым обучением в формальных учебных заведениях и корпоративном обучении. Существует широкий спектр инструментов для цифрового обучения. Однако учащиеся и преподаватели должны владеть цифровой грамотностью, чтобы встретить эту новую эру в образовании. Что касается возможностей, необходимых для инструментов электронного обучения, эти инструменты должны обеспечивать равные возможности обучения для всех студентов. Включая людей с ограниченными возможностями, в развивающихся странах мало людей с ненадежным подключением к Интернету и электронными устройствами. Электронное обучение стало распространенным во многих странах мира из-за вспышки COVID-19. Таким образом, безопасность некоторых платформ электронного обучения является важным вопросом. В этом документе указаны проблемы безопасности, связанные с некоторыми электронными платформами для обучения, такими как Moodle, Zoom, Blackboard и edX. Кроме того, описаны многие виды кибератак из внешней сети на системы электронного обучения. Он также предоставляет лучшие практики по устранению угроз безопасности и кибератак на системы электронного образования. Примечательно, что механизм криптографии является лучшим методом защиты конфиденциальности, целостности и аутентификации (CIA) данных на электронных платформах. Однако видно, что один метод недостаточно силен, чтобы противостоять всей системе. Как следствие, необходимо сочетать различные методы, такие как биометрическая аутентификация, межсетевые экраны, IDS, цифровые водяные знаки и модели процессов безопасности с различными уровнями стандартов безопасности для управления и контроля процессов обработки данных в системах электронного обучения для смягчения проблем кибербезопасности и кибератак.

Литература

1. Li, C., & Lalani, F. (2020, April 29). The rise of online learning during the COVID-19 pandemic. World Economic Forum. https://www.weforum.org /agenda/2020/04/coronaviruseducation-global-covid19-online-digital-learning/

2. Mawgoud, A.A., Taha, M.H.N., & Khalifa, N.E.M. (2020). Security Threats of Social Internet of Things in the Higher Education Environment. Studies in Computational Intelligence, 846, 151–171. https://doi.org/10.1007/978-3-030-24513-9_9.

3. Serhan, D. (2020). Transitioning from Face-to-Face to Remote Learning: Students' Attitudes and Perceptions of using Zoom during COVID-19 pandemic. International Journal of Technology in Education and Science, 4(4), 335–342. https://doi.org/10.46328/IJTES.V4I4.148.

4. Olaza-Maguiña, A.F., & De La Cruz-Ramirez, Y.M. (2021). Digital Education and Information Security in Obstetric Students in COVID-19 Pandemic Times in Peru. 97–107. https://doi.org/10.1007/978-3-030-85893-3_7

5. Kumar, S., & Dutta, K. (2011). Investigation on security in LMS moodle. International Journal of Information Technology …, 4(1), 233–238.

6. Matt Miller. (2020). Zoom security issues.

7. Charlie Osborne. (2021). Critical Zoom vulnerability triggers remote code execution without user input.

8. Paul Wagenseil. (2021). Zoom security issues: Here's everything that's gone wrong (so far).

9. Ahmed, R. (2020). Zoom Vulnerabilities Demonstrated in DEF CON Talk.

10. M.V. Eekelen, R. Moussa, Engelbert Hubbers, & Roel Verdult. (2013). Blackboard Security Assessment. CTIT Technical Report Series, April.

11. Fayziyeva, D. S., Yuldasheva, N.S., & Ugli, I.S.Z. (2019). Security issues in E-Learning system. International Conference on Information Science and Communications Technologies: Applications, Trends, and Opportunities, ICISCT 2019, April. https://doi.org/10.1109/ICISCT47635.2019.9011971.

DIGITAL EDUCATION: SECURITY ISSUES AND BEST PRACTICES

Sh.Y.Kholov

Tajik Technical University named after. Academician M.S. Osimi, Dushanbe, Tajikistan, sh.kholov88@gmail.com

Abstract. As a result of this research, cryptographic mechanism emerges as the best method for protecting confidentiality, authentication, and authentication (CIA) of data on electronic platforms. However, it is not strong enough to mitigate cybersecurity. For this reason, it is intended that the encryption mechanism should not be combined with other methods such as biometric authentication, firewalls, IDS, digital watermarking, and process models.

Keywords. Digital education, security, problems, measures.