В. С. Литвинова, Н. Е. Губенко
Донецкий национальный технический университет, г. Донецк
УДК 004.056

ИСПОЛЬЗОВАНИЕ ИННОВАЦИОННЫХ ТЕХНОЛОГИЙ ДЛЯ ПОВЫШЕНИЯ КИБЕРБЕЗОПАСНОСТИ ОБРАЗОВАТЕЛЬНЫХ ВЕБ-РЕСУРСОВ

Аннотация. В работе исследуются инновационные технологии, которые можно использовать для усиления мер кибербезопасности на образовательных платформах. Рассматриваются проблемы, с которыми сталкиваются образовательные учреждения при защите конфиденциальных данных и обеспечении бесперебойного доступа к учебным материалам.

Ключевые слова: инновационные технологии, кибербезопасность, веб-ресурс, образование, программное обеспечение, кибератака, искусственный интеллект.

Введение. В современном мире наблюдается тенденция [1, 2] к дигитализации всех сфер жизни, включая и сферу образования. Образовательные учреждения все чаще начинают использовать цифровые технологии в учебном процессе, предоставляя доступ обучающимся к различным образовательным ресурсам в глобальной сети. Такие ресурсы, как электронные библиотеки, онлайн-курсы и видеоуроки, позволяют студентам получать знания и навыки в любое время, не зависимо от местонахождения.

Однако данная цифровая трансформация в образовательных веб-ресурсах тесно сопряжена с рисками кибератак, которые могут привести к утечке конфиденциальной информации, нарушению работы системы и множеством негативных последствий. Кибератаки в свою очередь, не только ставят под угрозу конфиденциальные данные, но и нарушают непрерывность учебной деятельности.

Источник угрозы [3] — потенциальные антропогенные, техногенные или стихийные носители угрозы безопасности. Уязвимость — слабый компонент ИС, который приводит к нарушению безопасности информации, обусловленный недостатками процесса функционирования объекта.

Проблема исследования. В последнее время разработчики образовательных веб-ресурсов часто сталкиваются с многочисленными проблемами при обеспечении надежной кибербезопасности создаваемых проектов [4, 5]. Эти проблемы включают в себя уязвимости в программном обеспечении, используемом для онлайн-обучения, некорректные механизмы аутентификации пользователей и контроля доступа, отсутствие комплексных стратегий защиты данных, а также постоянные угрозы, такие как фишинговые атаки и проникновение вредоносных программ.

Угроза — это потенциальная опасность, которая может возникнуть в информационной системе, если нарушитель использует ее уязвимости для атак. Вероятность реализации, уровень ущерба и степень риска угроз является важной составляющей при анализе проблем кибербезопасности образовательных веб-ресурсов и их решения (см. табл. 1).

Анализ предоставленной информации (см. табл. 1) позволяет сделать вывод о том, что на сегодняшний день существует разнообразие угроз, поэтому необходимо уделить внимание профилактике уязвимостей, разработке мер по предотвращению угроз, обучению сотрудников и студентов правилам безопасности, а также регулярному мониторингу и обновлению системы защиты информации.

Таблица 1

Перечень возможных угроз кибербезопасности

Угроза	*Вероятность реализации*	*Уровень ущерба*	*Степень риска*
Несанкционированный доступ к стратегической информации	Низкий	Высокий	Средний
Кража документации	Средний	Высокий	Высокий
Несанкционированный доступ к конфиденциальной информации	Низкий	Высокий	Средний
Утечка данных (распространение персональных данных)	Средний	Высокий	Высокий
Утечка данных (разглашение юридической тайны)	Низкий	Высокий	Средний
Уничтожение файлового сервера	Низкий	Высокий	Средний
Стихийные угрозы	Высокий	Умеренный	Средний
Слишком большой объем данных	Высокий	Низкий	Средний
Неисправное оборудование	Средний	Умеренный	Средний
Заражение системы вирусом	Низкий	Высокий	Средний

Также важно отметить, что вероятность реализации угрозы и степень риска также играют ключевую роль в анализе кибербезопасности. Низкая вероятность реализации угрозы не должна быть воспринята как незначительная, особенно при высоком уровне ущерба.

Материалы и методы. Исходя из вышесказанного владельцам и администраторам образовательных веб-ресурсов следует серьезно отнестись к обеспечению кибербезопасности [6], учитывая разнообразие угроз и их потенциальные последствия для образовательного процесса.

Благодаря совершенствованию знаний в области инновационных технологий и их использования, появляется возможность эффективного применения современных средств и методов для повышения кибербезопасности образовательных веб-ресурсов. Развитие новых технологий, таких как искусственный интеллект, машинное обучение, блокчейн и другие, предоставляет широкий спектр разнообразных инструментов для обнаружения, предотвращения и реагирования на угрозы безопасности информации.

Решение проблем кибербезопасности на базе искусственного интеллекта предлагает возможность обнаружения и смягчения угроз. Алгоритмы машинного обучения могут анализировать огромные объемы данных для выявления аномальных моделей поведения, указывающих на кибератаки. Кроме того, механизмы аутентификации на основе искусственного интеллекта улучшают процессы проверки всех пользователей веб-ресурса, сводя к минимуму риск несанкционированного доступа к образовательной платформе.

В свою очередь технология блокчейн является не менее актуальной и востребованной в сфере киберзащиты, она способна обеспечить децентрализованный и неизменяемый реестр для безопасной записи транзакций и передачи данных. Внедряя протоколы аутентификации и авторизации на основе блокчейн, образовательные учреждения могут создавать защищенные записи о действиях пользователей, а также быть уверенными в целостности академических полномочий и сертификатов.

Результаты. Разработчики образовательных веб-сайтов должны принять стандартные рекомендации по написанию скриптов и регулярно обновлять программные компоненты для устранения известных уязвимостей безопасности.

Таким образом благодаря использованию инновационных технологий и их интеграции в единую структуру может значительно повысить кибербезопасность образовательных веб-ресурсов. В результате мы получаем многофункциональную систему обнаружения и реагирования на угрозы на базе искусственного интеллекта, а также систему аутентификации и управления учетными данными на основе блокчейна.

Заключение. В заключение следует отметить, что защита образовательных веб-ресурсов от киберугроз требует внедрения инновационных технологий, адаптированных к уникальным требованиям сектора образования. Применяя искусственный интеллект, блокчейн и методы безопасного кодирования, образовательные учреждения могут укрепить свою позицию в области кибербезопасности и обеспечить целостность и доступность онлайн-обучающих материалов.

Поскольку цифровой ландшафт продолжает развиваться, постоянные исследования и сотрудничество необходимы, чтобы опередить возникающие киберугрозы и защищать будущее онлайн-образования.

СПИСОК ЛИТЕРАТУРЫ

1. Руденко Л.И. Моделирование оценки рисков информационной безопасности / И.Л. Руденко, Е.В. Пушкарева // Всероссийская с международным участием научно-практическая конференция, Крымский федеральный университет имени В. И. Вернадского. 2019. — С. 163-165.
2. Способы защиты информации // «Серчинформ»: сайт. — URL: https://searchinform.ru/informatsionnaya-bezopasnost/zaschita-informatsii/sposoby-zaschity-informatsii.
3. Петраков А.В. Основы практической защиты информации: учебное пособие. — Москва, 2005. — 281 с.
4. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. — Санкт-Петербург, 2004. — 384 с.
5. Классификация источников угроз // Классификация источников угроз. — 2019. — URL: https://vuzlit.ru/963945/klassifikatsiya_istochnikov_ugroz — загл. с экрана.
6. Стандарты информационной безопасности // Информация о стандартах информационной безопасности. — 2019. — URL: https://arinteg.ru/articles/standarty-informatsionnoybezopasnosti 27697.html.