

УДК 004

Разработка политики информационной безопасности для образовательной игры

Ашрафи Арифа ^(*)	arifaa13@gmail.com
Мохначев Виктор Сергеевич	gagashaggy@inbox.ru SPIN-код: 1863-0407
Филиппович Юрий Николаевич	y_philippovich@mail.ru SPIN-код: 1660-0675
Махмуд Али Айманович	makhmud_ali22@mail.ru
Мехрез Мохаммад	mohamad.mehrez@mail.ru

Московский политехнический университет, Москва, Россия

Аннотация. В статье рассматриваются критические проблемы информационной безопасности в образовательном ПО, в частности — уязвимости на стороне клиента, ведущие к нарушению целостности данных и конфиденциальности. В качестве решения предлагается проактивный подход, основанный на приоритете разработки комплексной Политики информационной безопасности над точечными исправлениями. Методология апробирована на примере образовательной игры: с помощью статического анализа кода на основе ИИ и динамического сканирования был проведен аудит исходной кодовой базы, выявивший 100 % успешных манипуляций. В ответ была разработана и внедрена Политика, предписывающая переход к серверно-ориентированной архитектуре, основанной на принципах нулевого доверия. Результаты подтверждают, что только интеграция строгой политики, автоматизированных инструментов и процессов разработки обеспечивает создание безопасных и надежных образовательных технологий.

Ключевые слова: политика информационной безопасности, образовательные технологии, разработка безопасного программного обеспечения, безопасность на стороне клиента, целостность данных, контроль доступа, GDPR (Общий регламент по защите данных), разработка игр

Введение. Исходная кодовая база образовательной игры, разработанной в рамках многоязычной платформы для изучения языка жестов [1], содержала критические уязвимости безопасности, обусловленные изначальным доверием к клиентской среде, а именно: хранение всего состояния игры [2] (включая `unlockedLevels`, `completedLevels` и `inventory object`) в `localStorage` браузера; динамическое формирование URL без надлежащей валидации (например, `window.location.href = \levels/${lang}.html`); полное отсутствие серверных проверок безопасности; реализация контроля доступа исключительно на клиентской стороне через CSS-классы (например, `.locked`).

Материалы и методы; результаты. Для устранения выявленных уязвимостей была разработана и реализована серверно-ориентированная архитектура безопасности. Ключевые меры включали перенос данных и бизнес-

логики на сервер с использованием защищенных API-вызовов (GET/POST /api/progress), внедрение многоуровневой валидации и аутентификации на основе JWT-токенов. Реализованный подход устранил ключевые уязвимости (CWE-602, CWE-116), значительно повысив защищенность приложения.

Оценка эффективности с помощью симуляций атак и практического проекта со студентами показала значительное снижение количества уязвимостей: на 92 % в моделях и на 85 % в реальном коде.

Заключение. Данное исследование демонстрирует эффективность проактивного подхода к обеспечению безопасности, основанного на политике. Внедрение формальной политики информационной безопасности позволило осуществить переход к безопасной серверной модели, основанной на принципах нулевого доверия. Эта трансформация привела к практически полному устранению наиболее критических уязвимостей (~93,3 %). Ключевым результатом является не только создание безопасной игры [3], но и разработка универсальной методологии, сочетающей технические меры с организационными.

Список источников

- [1] Ашрафи А., Мохначев В.С. Разработка удобных интерфейсов для многоязычного словаря жестового языка. *Искусственный интеллект в автоматизированных системах управления и обработки данных. II Всерос. науч. конф.: сб. ст.* Москва, КДУ, 2023, т. 1, с. 368–375.
- [2] Pauly M., Parikh R. Game Logic — an Overview. *Studia Logica*, 2003, vol. 75, pp. 165–182. <https://doi.org/10.1023/A:1027354826364>
- [3] Schrader C. Serious Games and Game-Based Learning. *Handbook of Open, Distance and Digital Education*. Singapore, Springer, 2023, pp. 1255–1268. https://doi.org/10.1007/978-981-19-2080-6_74