Секция «Компьютерное право и информационная безопасность»

# Обеспечение информационной безопасности системы распределения нагрузки преподавателей кафедры

**Научный руководитель – Дубровина Оксана Васильевна**

***Клейменов Анатолий Романович***
*Студент (бакалавр)*
Тамбовский государственный технический университет, Тамбовская область, Россия
*E-mail: kleimenovt@gmail.com*

Активное внедрение цифровых технологий в сферу образования в России делает вопросы информационной безопасности особенно актуальными. Сотрудникам университета, которые обрабатывают персональные данные, необходимо соблюдать требования Федерального закона № 152-ФЗ «О персональных данных», а также руководствоваться Федеральным законом № 273-ФЗ «Об образовании в Российской Федерации». Оба документа не только предусматривают ответственность за несанкционированное раскрытие персональных сведений, но и формируют конкретные требования к информационным системам, работающим с конфиденциальными данными [1].

Рассматриваемая информационная система кафедры предназначена для автоматизации распределения нагрузки преподавателей, формирования индивидуальных планов и отчетных документов. Хотя число пользователей (около тридцати преподавателей) не является большим, утечка данных может иметь крайне негативные последствия.

Авторизация в системе реализуется в рамках ролевой модели *RBAC* (*Role-Based Access Control*). Преподаватель, обладая минимальными привилегиями, видит и редактирует только собственную информацию, тогда как заведующий кафедрой имеет расширенные права, необходимые для управления всеми пользователями [2].

Для усиления уровня защиты учётных записей дополнительно применяется двухфакторная аутентификация. Она вводит во внутренний контур безопасности второй фактор – одноразовые коды, которые предлагается генерировать с помощью приложения Яндекс.Ключ.

Пароли пользователей хранятся в хешированном виде с использованием алгоритма *Argon*2*id*. Он обеспечивает высокую устойчивость к перебору, так как допускает гибкую настройку объёма памяти, числа итераций и параллелизма, что значительно усложняет задачу взлома для злоумышленников.

Все данные, передаваемые между клиентской частью и сервером, шифруются с помощью протокола *SSL*/*TLS*, что исключает вероятность перехвата или модификации трафика по схеме «человек посередине». Дополнительно обеспечивается контроль сессий и их своевременный отзыв. При бездействии пользователя в течение определённого периода происходит автоматический выход из системы, а в случае подозрения на утечку токена администратор может отозвать активную сессию. Механизм *Rate Limiting* предотвращает частые повторные попытки входа, тем самым затрудняя перебор пароля и снижая вероятность *DDoS*-атак, направленных на перегрузку сервера.

Для предотвращения *SQL*-инъекций и *XSS*-атак все входные данные проходят процедуру валидации. При необходимости отображать пользовательский контент в браузере применяется дополнительная очистка *HTML* (посредством библиотеки *DOMPurify*), исключающая внедрение вредоносных скриптов. Защита от *CSRF* осуществляется путём внедрения уникальных токенов в запросы, меняющие состояние системы, и использованием *HttpOnly cookies*, недоступных из клиентского *JavaScript*-кода [3].

При разработке системы используется *Docker* для контейнеризации сервисов. Такой подход повышает уровень изоляции и упрощает управление зависимостями. Для обнаружения проблем на уровне инфраструктуры дополнительно настраивается базовое журналирование событий, позволяющее выявлять подозрительные действия и предпринимать упреждающие меры безопасности. Неотъемлемым аспектом является организация резервного копирования базы данных, поскольку подобная практика позволяет восстановить работоспособность системы при сбоях или намеренных атаках. Создаваемые бэкапы надёжно шифруются алгоритмом *AES*-256 перед хранением, что сохраняет конфиденциальность данных даже при возможном несанкционированном доступе к архивам.

Таким образом, обеспечение информационной безопасности в образовательной сфере требует комплексного подхода. Внедрение современных методов защиты, таких как двухфакторная аутентификация, хеширование паролей и шифрование данных, минимизирует риски утечек.

**Источники и литература**

1) Исаев А.С., Хлюпина Е.А. «Правовые основы организации защиты персональных данных» – СПб: НИУ ИТМО, 2014. – 106 с.
2) Основы технологий баз данных: учебное пособие / Б. А. Новиков, Е. А. Горшкова, Н. Г. Графеева; под ред. Е. В. Рогова. — 2-е изд. — М.: ДМКПресс, 2020. —582с.
3) Щербак, А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — Москва : Издательство Юрайт, 2022. — 259 с.