УДК 004.42

ИССЛЕДОВАНИЕ МЕТОДОВ ЗАЩИТЫ ИНФОРМАЦИИ В ВЕБ-ПРИЛОЖЕНИИ ДЛЯ ЗАВЕДУЮЩЕГО ОБЩЕЖИТИЕМ

Кряжева Е.В.,

к. псих. н., доцент,

Калужский государственный университет им. К.Э. Циолковского,

Калуга, Россия

Лебедянцев С. П.,

магистрант,

Калужский государственный университет им. К.Э. Циолковского,

Калуга, Россия

Аннотация.

В условиях цифровизации образовательных учреждений вопросы защиты персональных данных становятся критически важными. Статья посвящена исследованию методов защиты информации в веб-приложении для заведующего общежитием. Проведен анализ предметной области, выполнен сравнительный анализ существующих информационных систем-аналогов с применением методов контент-анализа и экспертной оценки. Определены программно-технические средства реализации системы, изучены актуальные угрозы по методологии OWASP Top 10 и предложены способы их нейтрализации. Разработанный комплекс мер защиты включает шифрование чувствительных полей в базе данных (AES-256), двухфакторную аутентификацию на основе TOTP, подсистему аудита событий безопасности и настройку защитных HTTP-заголовков. Эффективность предложенных мер подтверждена с использованием OWASP ZAP.

Ключевые слова: защита персональных данных, веб-приложение, двухфакторная аутентификация, шифрование данных, сравнительный анализ, программно-технические средства.

RESEARCH OF INFORMATION PROTECTION METHODS IN A WEB APPLICATION FOR THE HEAD OF THE DORMITORY

Kryazheva E.V.,
Candidate of Psychology, Associate Professor,
K.E. Tsiolkovsky Kaluga State University,
Kaluga, Russia
Lebedyantsev S.P.,
Master's Student,
K.E. Tsiolkovsky Kaluga State University,
Kaluga, Russia

Annotation.
With the digitalization of educational institutions, personal data protection issues are becoming critical. This article examines information security methods in a web application for a dormitory manager. A domain analysis is conducted, along with a comparative analysis of existing comparable information systems using content analysis and expert evaluation. The software and hardware for implementing the system are identified, current threats are analyzed using the OWASP Top 10 methodology, and mitigation methods are proposed. The developed security measures include encryption of sensitive database fields (AES-256), TOTP-based two-factor authentication, a security event audit subsystem, and the configuration of secure HTTP headers. The effectiveness of the proposed measures was confirmed using OWASP ZAP.

Keywords: personal data protection, web application, two-factor authentication, data encryption, comparative analysis, software and hardware.

Современные образовательные учреждения активно внедряют автоматизированные информационные системы для управления различными аспектами деятельности, включая учет жилищного фонда. Процессы заселения, выселения, контроля проживающих студентов требуют обработки значительных объемов персональных данных (далее ПДн): фамилии, имена, отчества, учебные группы, контактные данные, история проживания.

Разработанное ранее веб-приложение для заведующего общежитием обеспечивало базовую автоматизацию учета, однако вопросы защиты персональных данных были реализованы на минимальном уровне (аутентификация по паролю, JWT-токены, CSRF-защита). Проведенный предварительный анализ выявил ряд уязвимостей, характерных для многих веб-приложений образовательных учреждений: хранение ПДн в открытом виде в базе данных, отсутствие двухфакторной аутентификации, недостаточная настройка защитных HTTP-заголовков.

Актуальность исследования обусловлена ужесточением требований регуляторов в области защиты персональных данных (152-ФЗ [1], Приказ ФСТЭК № 21 [2]), ростом числа кибератак на образовательные учреждения и необходимостью создания типового решения, масштабируемого на другие организации.

Для определения наиболее эффективных подходов к защите персональных данных в разрабатываемой системе был проведен сравнительный анализ существующих информационных систем, предназначенных для автоматизации управления жилищным фондом образовательных учреждений. В качестве объектов сравнения выбраны три системы:

1. «Университетское общежитие» (ООО «ИТ-Сервис») - коммерческое решение, ориентированное на крупные вузы.

2. «Dormitory Management System» (Open Source) - открытое решение, распространенное в зарубежных университетах.

3. «1С: Университет ПРОФ» - модуль управления общежитиями в составе платформы 1С.

Анализ проводился с использованием метода контент-анализа официальной документации и экспертной оценки по критериям безопасности. Результаты представлены в таблице 1.

Таблица 1 — Сравнительный анализ ИС - аналогов

Критерий	**«Университетское общежитие»**	**«Dormitory MS»**	**«1С: Университет ПРОФ»**	**Разрабатываемая система**
Шифрование данных хранения	Частичное (только резервные копии)	Отсутствует	Присутствует (на уровне СУБД)	Присутствует (AES-256, ORM)
Двухфакторная аутентификация	Отсутствует	Отсутствует	Присутствует (аппаратные ключи)	Присутствует (TOTP)
Подсистема аудита	Присутствует	Частично	Присутствует	Присутствует
Защитные HTTP-заголовки	Частично	Отсутствуют	Присутствуют	Присутствуют (CSP, HSTS, X-Frame-Options)
Соответствие 152-ФЗ	Частичное	Не соответствует	Соответствует	Соответствует

Результаты анализа показывают, что существующие аналоги либо не в полной мере соответствуют российским требованиям защиты ПДн, либо требуют

значительных затрат на внедрение. Разрабатываемая система сочетает функциональную полноту с реализацией всех необходимых мер защиты.

Для обеспечения требуемого уровня защищенности при сохранении производительности и масштабируемости выбраны следующие программно-технические средства (далее ПТС):

– Серверное программное обеспечение:

– Операционная система: Ubuntu Server 22.04 LTS — обеспечивает стабильность, регулярные обновления безопасности и совместимость с современными средствами защиты.

– Веб-сервер: Nginx — используется для проксирования запросов, настройки HTTPS и защитных HTTP-заголовков.

– СУБД: PostgreSQL 15 — обеспечивает надежное хранение данных, поддержку шифрования на уровне таблиц и детальную систему прав доступа.

– Платформа разработки: Python 3.10 + Flask — позволяет гибко реализовать шифрование на уровне ORM, интеграцию с библиотеками TOTP и подсистему аудита.

К клиентскому программному обеспечению относятся:

1) Веб-браузер с поддержкой современных стандартов безопасности (TLS 1.3, Content-Security-Policy).

2) Мобильное приложение-аутентификатор (Google Authenticator, Яндекс.Ключ) для реализации двухфакторной аутентификации.

Аппаратное обеспечение представлено:

1) Серверное оборудование с поддержкой аппаратного ускорения шифрования (AES-NI) для минимизации влияния криптографических операций на производительность.

2) Резервное копирование на защищенный сетевой накопитель с шифрованием.

Выбранные ПТС обеспечивают баланс между стоимостью внедрения, производительностью и уровнем защиты, а также полностью соответствуют требованиям нормативных документов.

На основе анализа предметной области и типовых архитектур веб-приложений, а также с использованием методологии OWASP Top 10:2021 [3] выявлены основные угрозы для разрабатываемой информационной системы. Для каждой угрозы (таблица 2) определен способ защиты, реализованный в системе.

Таблица 2 — Угрозы и способы защиты

Угроза (OWASP ID)	**Описание**	**Способ защиты**
A04:2021 — Insecure Design	Хранение персональных данных в открытом виде в базе данных; при физическом доступе к файлу базы данных злоумышленник получает полный доступ ко всем ПДн.	Шифрование полей full_name и group на уровне ORM с использованием AES-256-GCM. Ключ шифрования хранится в переменной окружения.
A07:2021 — Identification and Authentication Failures	Использование только парольной аутентификации; при компрометации пароля злоумышленник получает полный доступ к системе.	Внедрение двухфакторной аутентификации по протоколу TOTP (RFC 6238). При входе требуется пароль и 6-значный код из приложения-аутентификатора.
A05:2021 — Security Misconfiguration	Отсутствие защитных HTTP-заголовков, что увеличивает риски атак типа clickjacking, перехвата трафика, выполнения нежелательных скриптов.	Настройка заголовков: Content-Security-Policy, X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options. Принудительное использование HTTPS.
A09:2021 — Security Logging and Monitoring Failures	Отсутствие регистрации событий безопасности затрудняет обнаружение инцидентов и расследование нарушений.	Подсистема аудита с записью успешных/неуспешных входов, изменения пароля, включения/отключения 2FA, критических операций.

Результатом разработки являются:

1. *Реализованные механизмы защиты:*

Для шифрования данных на уровне ORM используется симметричное шифрование AES-256 в режиме GCM. Ключ шифрования хранится в переменной окружения. В SQLAlchemy реализован пользовательский тип данных EncryptedString, автоматически шифрующий значение при записи и дешифрующий при чтении. При попытке прямого доступа к файлу базы данных содержимое поля представлено в зашифрованном виде.

Двухфакторная аутентификация (TOTP) реализована согласно RFC 6238 [4] с использованием библиотеки pyotp. Пользователь привязывает мобильное приложение-аутентификатор, после чего при входе дополнительно вводит 6-значный код, меняющийся каждые 30 секунд. Модель пользователя дополнена полями otp_secret и is_2fa_enabled.

2. *Подсистема аудита.*

Создана модель SecurityLog, в которую записываются все значимые события безопасности. Журнал защищен от изменения и доступен только администратору.

3. *Защитные HTTP-заголовки.*

На уровне Nginx настроены:

```
add_header Content-Security-Policy "default-src 'self'" always;
add_header X-Frame-Options "DENY" always;
add_header Strict-Transport-Security "max-age=31536000; includeSubDomains" always;
add_header X-Content-Type-Options "nosniff" always;
```

4. *Оценка эффективности мер защиты*

Для оценки эффективности проведено тестирование с использованием инструмента OWASP ZAP [6] до и после внедрения защиты. Результаты можно увидеть в таблице 3.

Таблица 3 — Результаты тестирования OWASP ZAP

Категория уязвимости	**Исходная версия**	**Защищенная версия**
SQL Injection	2	0

Категория уязвимости	**Исходная версия**	**Защищенная версия**
XSS (Cross-Site Scripting)	3	1
Information Disclosure	4	0
Insecure Headers	5	0
Weak Authentication	3	0
Критические уязвимости	**8**	**1**

Снижение количества критических уязвимостей составило 87,5%.

Проведены замеры времени отклика ключевых операций (таблица 4). Увеличение времени аутентификации связано с проверкой TOTP-кода, остальные операции показали увеличение не более 12%, что не создает дискомфорта для пользователя.

Таблица 4 — Сравнение времени отклика

Операция	**Исходная версия, мс**	**Защищенная версия, мс**	**Увеличение, %**
Аутентификация	85	128	+50,6
Загрузка основной таблицы (100 записей)	210	235	+11,9
Сохранение изменений (10 строк)	180	198	+10,0
Импорт Excel (50 студентов)	1250	1380	+10,4

Таким образом, в ходе исследования решены поставленные задачи: выполнен анализ предметной области, проведен сравнительный анализ ИС-аналогов, определены программно-технические средства реализации, изучены актуальные угрозы и предложены способы защиты (шифрование AES-256,

двухфакторная аутентификация TOTP, подсистема аудита, защитные HTTP-заголовки). Эффективность разработанного комплекса мер подтверждена результатами тестирования OWASP ZAP: количество критических уязвимостей снижено на 87,5% при увеличении времени отклика не более чем на 12%. Предложенные решения могут быть масштабированы на другие веб-приложения образовательных учреждений, обрабатывающие персональные данные.

Библиографический список:

1. Российская Федерация. Законы. О персональных данных : Федеральный закон № 152-ФЗ. — Москва : Кремль, 2006.
2. ФСТЭК России. Приказ от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных». — Москва, 2013.
3. OWASP Foundation. OWASP Top 10:2021 : The Ten Most Critical Web Application Security Risks. — 2021. — URL: https://owasp.org/Top10/ (дата обращения: 20.03.2026).
4. RFC 6238. TOTP: Time-Based One-Time Password Algorithm. — IETF, 2011. — URL: https://tools.ietf.org/html/rfc6238 (дата обращения: 20.03.2026).
5. OWASP Foundation. OWASP Zed Attack Proxy (ZAP). — URL: https://www.zaproxy.org/ (дата обращения: 20.03.2026).
6. PyOTP. PyOTP — The Python One-Time Password Library. — URL: https://github.com/pyauth/pyotp (дата обращения: 20.03.2026).
7. Dworkin, M. Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC / M. Dworkin // NIST Special Publication 800-38D. — 2007.