УДК 004.056.53

СИСТЕМА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОГО ОБМЕНА И УПРАВЛЕНИЯ ДОСТУПОМ К КОРПОРАТИВНЫМ ДОКУМЕНТАМ

Гичан А.Р.

Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь

Научный руководитель: Бобровничая М.А. – ст. преподаватель кафедры ИПиЭ

Аннотация. В работе рассматривается разработка системы безопасного обмена и управления доступом к корпоративным документам с использованием современных криптографических методов. Целью является обеспечение конфиденциальности, целостности и подлинности информации при хранении и передаче файлов. Особое внимание уделяется ролевой модели доступа, контролю версий и аудиту действий пользователей.

Ключевые слова: безопасный обмен, управление доступом, криптография, ролевая модель, контроль версий, аудит действий, *Django*, *Next.js*, *PostgreSQL*, *AES*, *RSA*

Введение. Задача обеспечения безопасного хранения и обмена файлами возникла с появлением Интернета. Основное внимание уделяется защите данных при хранении на сервере с помощью шифрования, разграничения доступа и физической защиты. Безопасность передачи файлов обычно обеспечивается протоколом *HTTPS*, объединяющим *HTTP* и *SSL/TLS*. Протокол предполагает обязательную аутентификацию сервера, тогда как аутентификация клиента осуществляется по имени и паролю. Надежность такой аутентификации определяется длиной, сложностью и сменой паролей. Примерами средств обмена данными являются облачные хранилища, мессенджеры и электронная почта [1].

Однако эти средства не всегда обеспечивают необходимый уровень безопасности и удобства. Возможны ограничения по типу и размеру файлов, а также по объему хранилища. Использование ссылок повышает риск утечки информации, а ошибки пользователей могут привести к несанкционированному доступу. Кроме того, защита реализуется преимущественно на этапе передачи данных, тогда как безопасность хранении может быть недостаточной. Таким образом, возникает необходимость разработки специализированных систем, обеспечивающих конфиденциальность, целостность и подлинность информации.

Основная часть. В основе безопасного хранения и обмена файлами в сети Интернет лежат методы современной криптографии. В зависимости от задач и условий работы различают симметричные, асимметричные и комбинированные криптосистемы шифрования.

В симметричных криптосистемах используется один секретный ключ для шифрования и расшифрования. Данные криптосистемы характеризуются высокой скоростью шифрования и обеспечивают конфиденциальность, подлинность и целостность данных. Целостность достигается присоединением к данным специального кода (имитовставки). Асимметричные системы используют пару ключей: открытый для шифрования и секретный для расшифрования. Отправитель зашифровывает сообщение открытым ключом получателя, а расшифровать его может только владелец секретного ключа. Преимуществами таких систем являются решение проблемы распределения ключей и возможность взаимодействия не доверяющих сторон. К недостаткам относятся более низкая скорость работы и необходимость защиты открытых ключей от подмены.

Комбинированный подход сочетает преимущества обеих криптосистем. Симметричный алгоритм шифрует исходный текст, а ассиметричный – сеансовый ключ. Отправитель шифрует сообщение симметрично, затем зашифровывает сеансовый ключ открытым ключом получателя, который расшифровывает его своим секретным ключом и затем расшифровывает сообщение [2]. В разработанной системе был выбран именно комбинированный подход, объединяющий высокую скорость симметричного шифрования и безопасность передачи ключей. Для реализации такого подхода были выбраны алгоритмы *AES* и *RSA*. *AES* используется для симметричного шифрования, *RSA* для асимметричного.

Алгоритм *AES* представляет блок данных в виде двухмерного байтового массива и

выполняет несколько раундов преобразований: *ByteSub*, *ShiftRow*, *MixColumn* и *AddRoundKey*. Расшифрование выполняется обратными операциями. *AES* обеспечивает высокую скорость шифрования и минимальные требования к ресурсам. Алгоритм *RSA* основан на сложности факторизации больших чисел и использует пару ключей: открытый и секретный. Алгоритм эффективен для небольших сообщений, но значительно медленнее симметричных систем [2].

Для реализации системы была выбрана клиент-серверная архитектура. Серверная часть разработана с использованием *Django*, что позволило реализовать *API*, управление пользователями и хранение метаданных документов. Для хранения информации о документах, пользователях и ключах используется *PostgreSQL*, обеспечивающая надежность и поддержку сложных запросов. На рисунке 1 представлена структурная схема разработанной системы.

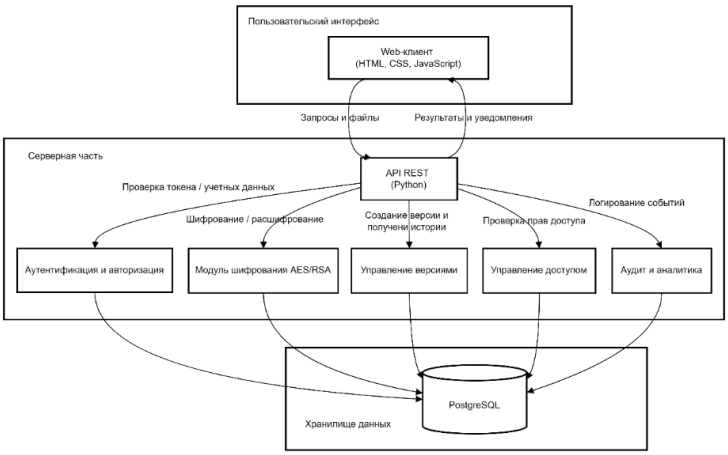

Рисунок 1 – Структурная схема системы обеспечения безопасного обмена и управления доступом к корпоративным документам

Для обеспечения надежности работы с документами реализован механизм контроля версий, дополняющий криптографическую защиту и позволяющий сохранять историю изменений, возвращаться к предыдущим версиям и определять автора изменений. Системы контроля версий широко используются в разработке программного обеспечения, а также при работе с большим количеством изменяющихся электронных документов [3].

При проектировании системы также необходимо было определить модель разграничения прав пользователей. Среди моделей политики безопасности традиционно выделяют дискреционную и мандатную. Дискреционная модель предполагает управление доступом субъектов к объектам через матрицу прав, а мандатная основана на присвоении субъектам и объектам классификационных меток, определяющих правила доступа. Однако существует также и ролевая модель, которая сочетает элементы обеих моделей и предполагает управление доступом через назначение ролей пользователям и соответствующих им прав [4]. В разработанной системе реализована ролевая модель, обеспечивающая централизованное администрирование прав и эффективное управление доступом к документам.

Для повышения безопасности в системе реализован механизм аудита действий пользователей. Все операции с документами и события фиксируются в журнале аудита, на основе которого формируется профиль. Он сравнивается с шаблоном нормального поведения, что позволяет выявлять аномалии и несанкционированные действия пользователей [5].

Клиентская часть системы реализована на основе *Next.js* и обеспечивает современный пользовательский интерфейс, удобный доступ к документам, их версиям и журналу аудита. Для визуализации работы с документами и результатами аудита предусмотрены динамические элементы и таблицы для наглядного представления информации. Интерфейс страницы управления документами представлен на рисунке 2.

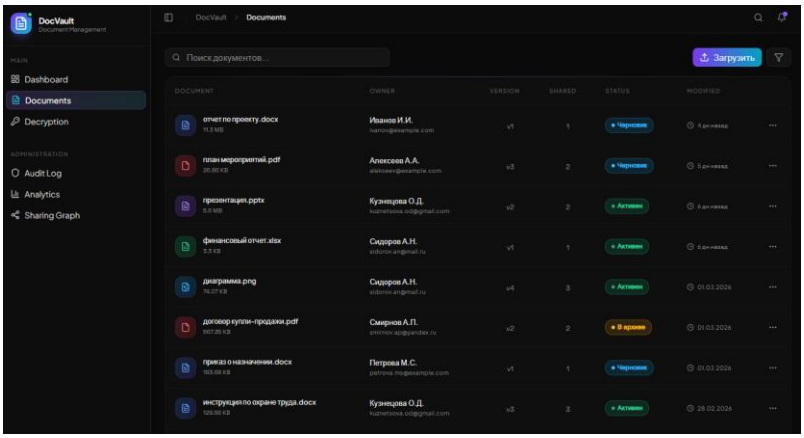

Рисунок 2 – Пользовательский интерфейс страницы управления документами

Взаимодействие клиента и сервера осуществляется через *REST API*, что позволяет фронтенду отправлять зашифрованные файлы, получать сеансовые ключи и актуальные версии документов, а также выполнять проверку прав доступа. Такой подход обеспечивает гибкость системы, масштабируемость и возможность интеграции с внешними сервисами.

Заключение. Разработанная система демонстрирует возможность интеграции современных криптографических методов с механизмами управления доступом и анализа активности пользователей. Применение комбинированного шифрования *AES* и *RSA* позволило объединить высокую скорость обработки данных с безопасной передачей ключей. Клиент-серверная архитектура обеспечивает гибкость взаимодействия пользовательского интерфейса и модуля обработки данных, а также централизованное хранение документов и управления их версиями. Ролевая модель доступа и аудит формируют контролируемую среду, позволяющую отслеживать действия пользователей. Таким образом, предложенный подход показывает эффективность сочетания криптографии, контроля версий и анализа активности при создании систем безопасного обмена документами в корпоративной среде.

Список литературы

1. *Хорев П.Б., Лосев Д.А. Безопасный обмен файлами на основе сетей доверия и сертификатов открытых ключей с помощью разработанного приложения // Программные продукты и системы. 2024. Т. 37. № 2. С. 230–237.*

2. *Информационная безопасность компьютерных систем и сетей: учебное пособие / В.Ф. Шаньгин. – Москва: ИД «ФОРУМ»: ИНФРА-М, 2020. – 416 с.*

3. *Васильева М.А. Система контроля версий. Основы командной разработки: учебное пособие / М.А. Васильева, К.М. Филипченко. – Санкт-Петербург: Лань, 2022. – 144 с.*

4. *Информационная безопасность и защита информации: учебное пособие / В.П.Мельников, С.А.Клейменов. – М.: Издательский центр «Академия», 2013. – 336 с.*

5. *Браницкий А.А., Котенко И.В. Анализ и классификация методов обнаружения сетевых атак.*

UDC 004.056.53

SYSTEM FOR SECURE EXCHANGE AND ACCESS MANAGEMENT TO CORPORATE DOCUMENTS

Gichan A.R.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Bobrovnichaya M.A. – senior lecturer at the department of EPE

Annotation. This paper examines the development of a system for secure exchange and access management of corporate documents using modern cryptographic methods. The goal is to ensure the confidentiality, integrity, and authenticity of information during file storage and transmission. Particular attention is paid to the role-based access model, version control, and user activity auditing.

Keywords: secure exchange, access control, cryptography, role-based model, version control, action auditing, Django, Next.js, PostgreSQL, AES, RSA