Развитие метода защиты конфиденциальных файлов в мессенджере на основе системы адаптивной аутентификации и блокирования при аномальной активности

И.В. Саварин
Финансовый университет при Правительстве Российской Федерации, Москва

Аннотация: В статье рассматривается развитие метода защиты конфиденциальных изображений в мессенджерах на основе маскирования ортогональными матрицами. Анализируется уязвимость системы к атакам перебора одноразовых паролей и компрометации учетных записей. Основное внимание уделено разработке архитектуры модулей анализа аномальной активности и адаптивной аутентификации. Представлена структура системы с независимыми компонентами безопасности, обеспечивающими блокировку при признаках атак полного перебора и гибкое управление сеансами доступа. Описано взаимодействие модулей в рамках единой системы безопасности с распределением функций между серверными и клиентскими компонентами.
Ключевые слова: Информационная безопасность, мессенджер, обмен сообщениями, коммуникации, системы мгновенного обмена сообщениями, аудит безопасности, атака перебора.

1. Введение

Современные мессенджеры стали неотъемлемой частью повседневной жизни и бизнеса, обеспечивая удобный и быстрый способ обмена информацией. Вместе с ростом популярности возрастает необходимость обеспечения надежной защиты передаваемых данных. Сравнительный анализ в исследовании [1] демонстрирует различные аспекты реализации механизмов защиты в корпоративных мессенджерах, выделяя их эффективные решения и потенциальные уязвимости. Одна из острых проблем заключается в хранении передаваемых данных в кэше файловой системы, что создает риск несанкционированного доступа. Для решения этой проблемы авторами статьи [2] предлагается использовать технологию маскирования изображений с помощью ортогональных преобразований, дополняющую существующие методы защиты. Предложенный метод маскирования с использованием ортогональных матриц, в частности, алгоритма Хилла, позволяет эффективно решить эту проблему, преобразуя изображение в нечитаемый вид до момента его открытия легитимным получателем. Однако обеспечение конфиденциальности данных не

ограничивается только защитой файла на диске. Не менее важным является контроль доступа к самому функционалу приложения. Еще одной мерой повышения безопасности передаваемых данных является внедрение дополнительного фактора аутентификации, например, одноразовых паролей основанных на времени (Time-based One-Time Password – TOTP), который значительно усиливает защиту конфиденциальной информации [3]. Тем не менее, этот подход имеет свои ограничения, включая риски атак методом перебора, хотя в TOTP они существенно ниже по сравнению с одноразовыми паролями на основе секрета (HMAC-Based One-Time Password) благодаря ограниченному времени жизни кода [4]. Основное же внимание следует уделить недостатку инструментов проактивного мониторинга подозрительной активности. Однако угроза аутентификации пользователя, в частности, подбор одноразового пароля (One-time password – OTP), используемого для подтверждения действий с конфиденциальными изображениями, представляет собой серьезный риск. С другой стороны, требование вводить одноразовый пароль при каждом обращении к одному и тому же изображению, будучи безопасным, создает избыточную нагрузку на пользователя, снижая практическую ценность системы и ухудшая пользовательский опыт (User experience – UX [5]).

Таким образом, актуальной задачей является развитие метода путем создания системы управления доступом, которая будет реализовывать два ключевых функционала: автоматическое блокирование учетных записей при обнаружении признаков атаки на подлинность пользователя и внедрение адаптивного механизма аутентификации, снижающего нагрузку на легитимного пользователя при многократном обращении к защищенным данным.

Статья состоит из 4 разделов. Во втором разделе проанализирована проблема аутентификации в контексте защиты изображений, выявлены

угрозы, связанные с потенциальным подбором одноразового пароля и негативным влиянием частых запросов кода подтверждения на удобство использования системы. В третьем разделе представлено развитие метода за счет интеграции системы реактивного управления доступом, включающей модуль анализа аномальной активности и модуль адаптивной аутентификации с механизмом сеансовых токенов, представлены диаграммы состояний системы обработки событий, связанных с изменением контекста сессии. В четвертом разделе описана архитектура взаимодействия новых модулей безопасности с ранее разработанной системой маскирования изображений.

2. Анализ проблемы аутентификации в контексте защиты изображений

Несмотря на то, что метод маскирования ортогональными матрицами [2] обеспечивает сохранность содержимого изображения при компрометации устройства, он не защищает от компрометации учетной записи пользователя. Если злоумышленник получил доступ к учетным данным, следующей линией обороны становится механизм двухфакторной аутентификации, часто реализуемый посредством TOTP. TOTP является надежным механизмом двухфакторной аутентификации, основанным на генерации одноразовых паролей с привязкой к текущему времени [3]. Однако, как и любая система аутентификации, он подвержен определенным угрозам безопасности.

Стандартная процедура, при которой код запрашивается каждый раз при попытке доступа к конфиденциальным данным, уязвима к атакам грубой силы [6], особенно в случае, если система не ограничивает количество попыток ввода. Успешная атака приведет к тому, что злоумышленник получит доступ к функционалу демаскирования, сведя на нет все преимущества криптографического преобразования. С другой стороны, для

легитимного пользователя, который в рамках рабочего дня многократно обращается к одним и тем же конфиденциальным изображениям (например, к графикам или схемам), постоянный ввод пароля становится обременительным. Это может провоцировать пользователей на поиск обходных путей, например, сохранения изображений в незамаскированном виде в обход мессенджера, что вновь создает уязвимость.

Таким образом, несмотря на высокую криптографическую стойкость метода маскирования изображений ортогональными матрицами, его эффективность может быть существенно снижена при компрометации процедуры аутентификации пользователя. Выявленные угрозы, связанные с потенциальным подбором одноразового пароля и негативным влиянием частых запросов кода подтверждения на удобство использования системы, указывают на необходимость создания дополнительного защитного контура. Данный контур должен быть нацелен не только на парирование атак на этапе аутентификации, но и на обеспечение сбалансированного пользовательского опыта, исключающего побуждение легитимных пользователей к небезопасным практикам.

3. Развитие метода: интеграция системы анализа активности и адаптивной аутентификации

Предлагаемое развитие метода заключается во введении в архитектуру мессенджера, описанную в предыдущей работе, двух серверных модулей:

1. Модуль анализатор аномальной активности.
2. Модуль адаптивной аутентификации.

Первый модуль, анализатор аномальной активности, непрерывно обрабатывает поток событий, связанных с вводом OTP. Его алгоритм основан на отслеживании частоты и источников неудачных попыток аутентификации. При превышении заданного порога (например, пять

неудачных попыток за три минуты с одного IP-адреса или для одной учетной записи) система автоматически блокирует возможность ввода OTP для данного источника на определенный период. Это делает бессмысленной атаку грубой силы, так как противник лишается возможности осуществлять перебор. Важно отметить, что данная блокировка не затрагивает возможность отправки сообщений в незащищенном режиме, что минимизирует ущерб для пользователя в случае ложного срабатывания, но надежно защищает доступ к критически важному функционалу демаскирования.

Второй модуль реализует механизм адаптивной аутентификации. После успешного ввода OTP для доступа к конкретному защищенному изображению система создает для данного пользователя и устройства безопасный сеансовый токен (Json Web Token [7]) с ограниченным временем жизни. В течение срока действия этого токена повторный доступ к тому же изображению или к другим изображениям от того же отправителя осуществляется без повторного запроса OTP. Это возможно потому, что клиентское приложение предъявляет серверу gRPC [8] валидный сеансовый токен. Также, критически важным элементом системы является непрерывный мониторинг параметров пользовательской сессии на предмет нетипичных изменений. В случае обнаружения событий, указывающих на потенциальный риск компрометации сессии – таких как смена IP-адреса пользователя, значительное изменение геолокации, явный перелогин в приложение или истечение установленного временного интервала безопасности – сеансовый токен немедленно терминируется. Это вызывает обязательный повторный запрос OTP при следующей попытке доступа к защищенному контенту, обеспечивая тем самым дополнительный уровень проверки подлинности пользователя. Такой подход кардинально улучшает удобство, сохраняя при

этом высокий уровень безопасности, поскольку первоначальный доступ был строго аутентифицирован.

Архитектура системы может быть представлена в виде диаграмм состояния [9], отражающих процесс аутентификации и проверки доступа (рис. 1), процесс верификации OTP и создания токена (рис. 2), процесс получения ключа демаскирования (рис. 3).

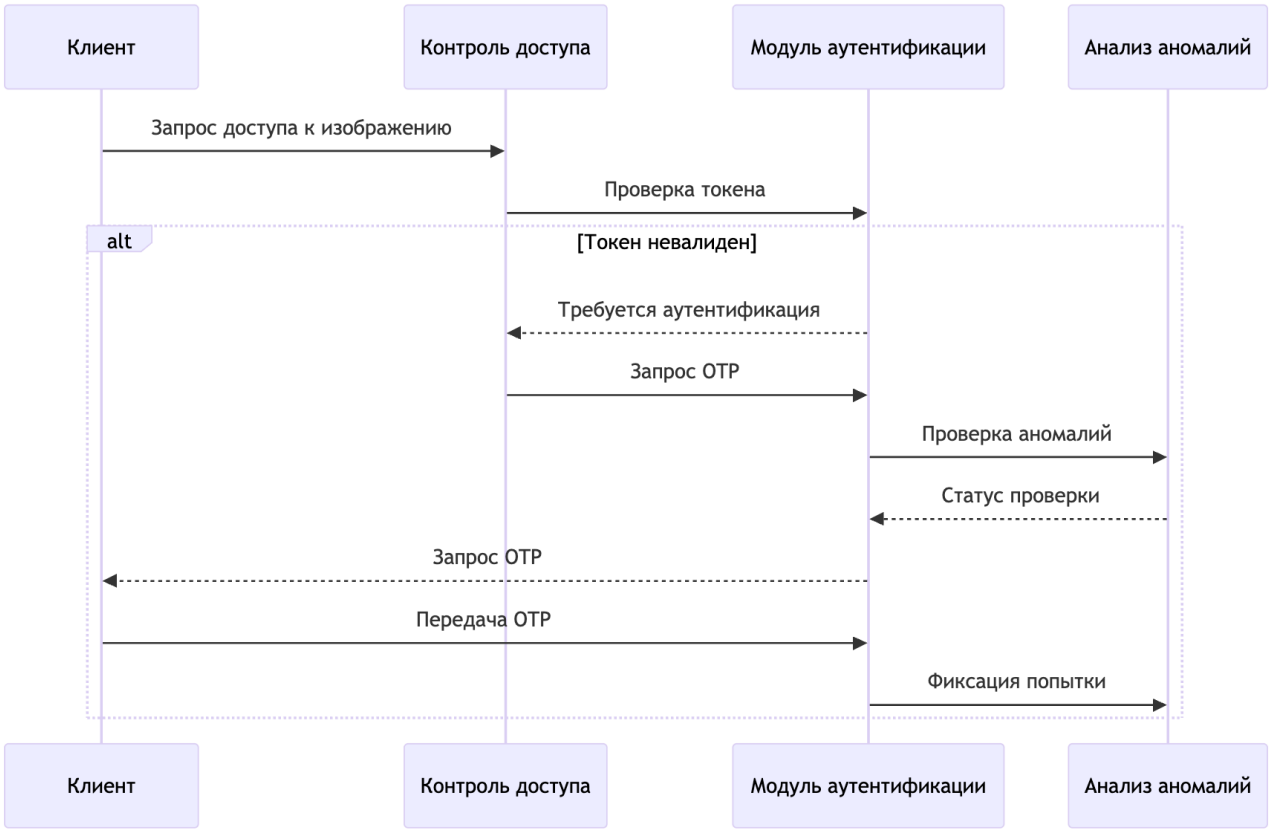

Рис. 1. – Процесс аутентификации и проверки доступа

Взаимодействие модулей безопасности происходит по следующей схеме: запрос на доступ к изображению от клиентского приложения поступает на модуль контроля доступа, который проверяет наличие действующего сеансового токена. При отсутствии токена или при наличии признаков риска (смена IP, геолокации и т.д.) запрос перенаправляется в модуль аутентификации, требующий ввод OTP. Успешная аутентификация инициирует создание токена и передачу обратной матрицы модулю маскирования/демаскирования, который, выполняет преобразование

изображения. Все события (успешные и неудачные попытки аутентификации, изменения сессии) фиксируются модулем анализа аномалий, который в реальном времени может инициировать блокировку сессии или учетной записи при превышении пороговых значений аномальной активности. Данная архитектура обеспечивает сквозной контроль безопасности на всех этапах работы с конфиденциальными изображениями.

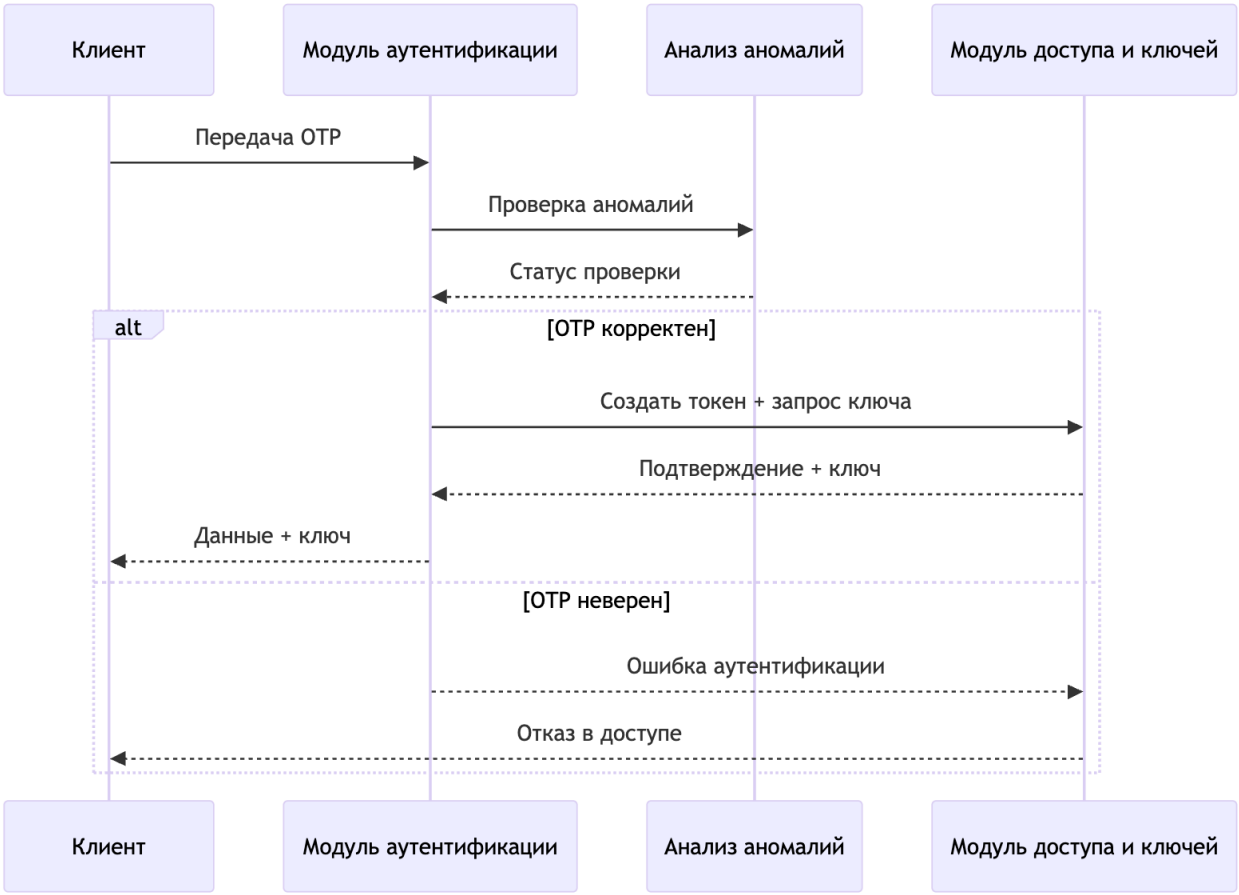

Рис. 2. – Процесс верификации OTP и создания токена

4. **Взаимодействие с системой маскирования изображений**

Предлагаемые модули анализа аномальной активности и адаптивной аутентификации реализованы в виде независимых сервисов, взаимодействующих с основной системой через четко определенные интерфейсы прикладного программирования (application programming interface – API [10]).

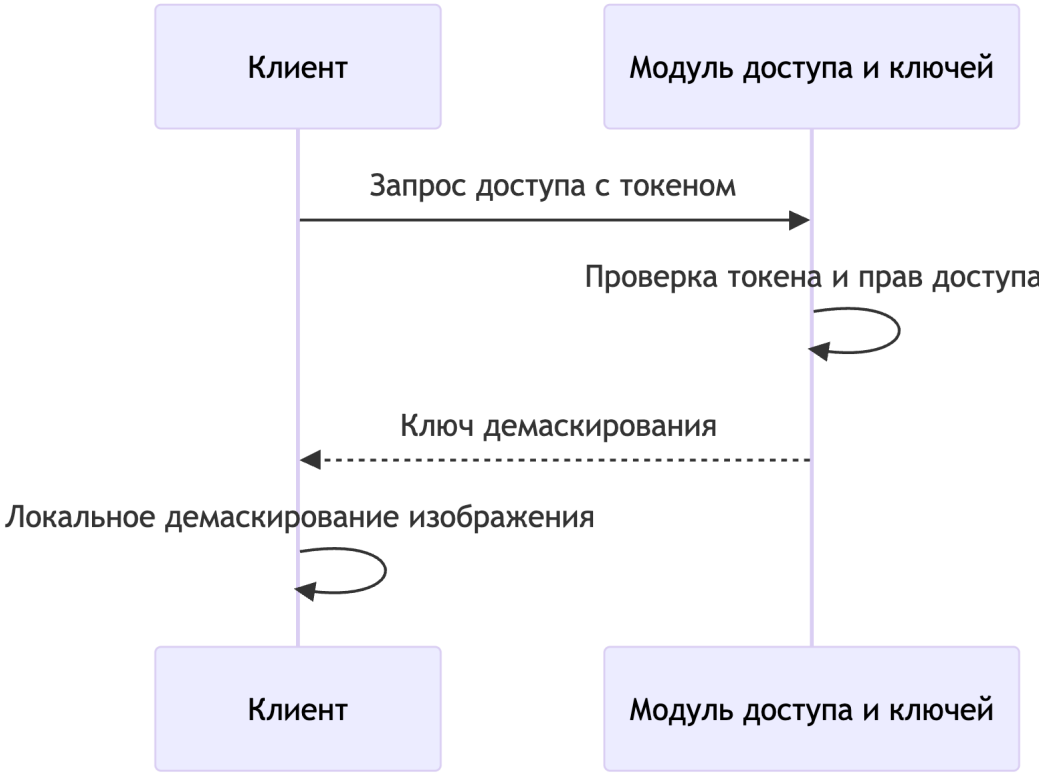

Рис. 3. – Процесс получения ключа и демаскирования

Такой подход обеспечивает возможность их отключения или изоляции в случае сбоев без нарушения работоспособности базового функционала мессенджера, связанного с передачей и получением сообщений. В штатном режиме работы решение о блокировке, сгенерированное анализатором аномальной активности, передается через API-шлюз в модуль обработки gRPC-запросов. Это предотвращает любые попытки аутентификации или доступа к ключам со стороны заблокированного пользователя или IP-адреса на самом раннем этапе, экономя вычислительные ресурсы.

Механизм адаптивной аутентификации функционирует как отдельный сервис управления сессиями. Прежде чем сервер обработает запрос на предоставление ключа демаскирования, он асинхронно проверяет валидность и контекст сеансового токена в этом сервисе. В случае несоответствия токена политикам безопасности (например, при смене геолокации) сервис сессий инвалидирует токен, и сервер отклоняет запрос на ключ. Важно подчеркнуть, что конечная операция демаскирования изображения выполняется

исключительно на стороне клиентского приложения. Сервер лишь предоставляет легитимному пользователю ключ (параметры обратной ортогональной матрицы) после успешного прохождения всех проверок, а применение этого ключа к замаскированным данным происходит локально на устройстве пользователя. Это не только повышает безопасность, исключая передачу восстановленного изображения по сети, но и распределяет вычислительную нагрузку. Таким образом, интеграция независимых модулей безопасности создает отказоустойчивый и масштабируемый контур защиты, не нарушающий базовую функциональность системы в случае необходимости временного отключения одного из компонентов.

Заключение

В рамках развития метода защиты конфиденциальных изображений в мессенджерах предложен и теоретически обоснован комплекс мер, направленных на усиление контроля доступа. Интеграция системы анализа аномальной активности и адаптивной аутентификации позволяет эффективно противостоять атакам на подлинность пользователя, что является критически важным дополнением к криптографическому методу маскирования ортогональными матрицами. Одновременно с этим достигается разумный баланс между безопасностью и удобством использования, что является ключевым фактором для внедрения подобных решений в практику. Предложенное развитие метода формирует целостный многоуровневый контур безопасности, устойчивый к широкому спектру угроз.

Литература

1. Коренева А. М., Саварин И. Сравнительный обзор безопасности популярных корпоративных мессенджеров // Инженерный вестник Дона, 2024, №8. URL: ivdon.ru/ru/magazine/archive/n8y2024/9416

2. Саварин И.В. Метод защиты изображений, передаваемых через мессенджер // Инженерный вестник Дона, 2024, №. 12. URL: ivdon.ru/ru/magazine/archive/n12y2024/9726

3. Саварин И.В. Метод повышения безопасности передачи изображений в мессенджерах с использованием одноразовых паролей // Инженерный вестник Дона, 2025, №. 1. URL: ivdon.ru/ru/magazine/archive/n1y2025/9799

4. Lumburovska, L., Dobreva, J., Andonov, S., Trpcheska, H. M., Dimitrova, V. A Comparative Analysis of HOTP and TOTP Authentication Algorithms. Which one to choose? // Security & Future, 2021, – Т. 5. – №. 4. – pp. 131-136.

5. Что такое UX/UI дизайн на самом деле? // Хабр. URL: habr.com/ru/articles/321312 (дата обращения: 03.10.2025).

6. Ayankoya F., Ohwo B. Brute-force attack prevention in cloud computing using one-time password and cryptographic hash function // International Journal of Computer Science and Information Security (IJCSIS), 2019. – Т. 17. – №. 2. – pp. 7-19.

7. Jones M., Bradley J., Sakimura N. Json web token (jwt). – 2015. – № rfc7519, pp. 4-5.

8. What is grpc // URL: grpc.io/docs/what-is-grpc/introduction/ (дата обращения: 03.10.2025)

9. Bell D. UML's sequence diagram // IBM. [Online] IBM. – 2004. – Т. 16. – №. 02. – pp.2-3.

10. Глава 1. Введение в API-интерфейсы для самых маленьких // URL: habr.com/ru/articles/890158 (дата обращения: 03.10.2025).

References

1. Koreneva A. M., Savarin I. Inzhenernyi vestnik Dona. 2024. №. 8. URL: ivdon.ru/ru/magazine/archive/n8y2024/9416

2. Savarin I.V. Inzhenernyi vestnik Dona, 2024, №. 12. URL: ivdon.ru/ru/magazine/archive/n12y2024/9726

3. Savarin I.V. Inzhenernyi vestnik Dona, 2025, №. 1. URL: ivdon.ru/ru/magazine/archive/n1y2025/9799

4. Lumburovska, L., Dobreva, J., Andonov, S., Trpcheska, H. M., Dimitrova, V. A Comparative Analysis of HOTP and TOTP Authentication Algorithms. Which one to choose, 2021: V.5. №.4. p.131-136

5. Chto takoe UX/UI dizajn na samom dele? URL: habr.com/ru/articles/321312 (date accessed: 03.10.2025).

6. Ayankoya F., Ohwo B. Brute-force attack prevention in cloud computing using one-time password and cryptographic hash function, 2019: V.17. №.2. pp.7-19

7. Jones M., Bradley J., Sakimura N. Json web token (jwt). 2015. № rfc7519. p.4-5

8. What is grpc URL: grpc.io/docs/what-is-grpc/introduction/ (date accessed: 03.10.2025).

9. Bell D. UML's sequence diagram, 2004. V. 16. №. 02. p.2-3

10. Glava 1. Vvedenie v API-interfejsy` dlya samy`x malen`kix [Chapter 1. Introduction to APIs for the youngest]. URL: habr.com/ru/articles/890158 (date accessed 03.10.2025).

Дата поступления: 14.09.2025

Дата публикации: 28.10.2025