УДК 004.7:35.08
DOI 10.33764/2618-981X-2025-6-172-175

Д. Х. Таргын[1]✉, И. Н. Карманов[1]

Методы аутентификации и авторизации в государственных приложениях

[1]Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: dtargyn02@mail.ru

Аннотация. В статье рассматриваются современные методы аутентификации и авторизации, применяемые в государственных приложениях для обеспечения безопасности данных. Особое внимание уделено многофакторной аутентификации и биометрическим технологиям. Анализируются преимущества и недостатки различных подходов, а также их соответствие требованиям информационной безопасности. Приводятся примеры успешного внедрения данных технологий в государственном секторе.

Ключевые слова: аутентификация, авторизация, многофакторная аутентификация, биометрия, государственные приложения, информационная безопасность

D. H. Targyn[1]✉, I. N. Karmanov[1]

Methods of authentication and authorization in government applications

[1]Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: dtargyn02@mail.ru

Abstract. The article examines modern authentication and authorization methods used in government applications to ensure data security. Particular attention is paid to multi-factor authentication and biometric technologies. The advantages and disadvantages of various approaches, as well as their compliance with information security requirements, are analyzed. Examples of successful implementation of these technologies in the public sector are given.

Keywords: authentication, authorization, multi-factor authentication, biometrics, government applications, information security

Введение

Государственные приложения обрабатывают конфиденциальные данные граждан, включая персональные, финансовые и медицинские сведения. Утечка или несанкционированный доступ к такой информации могут привести к серьезным последствиям, включая финансовые потери и угрозы национальной безопасности.

В связи с этим, разработка надежных методов аутентификации и авторизации становится важной задачей. Современные технологии, такие как многофакторная аутентификация (МФА), биометрия и децентрализованные системы, позволяют значительно повысить уровень защиты

Цель данной статьи – проанализировать актуальные методы аутентификации и авторизации, применяемые в государственных приложениях, оценить их эффективность и перспективы развития.

Однофакторная и многофакторная аутентификация

Аутентификация пользователей является фундаментальным элементом защиты информационных систем, особенно в государственном секторе, где обрабатываются конфиденциальные данные граждан. Исторически первой и наиболее распространенной формой аутентификации остается однофакторная система, основанная на связке логина и пароля. Однако, традиционная однофакторная аутентификация уязвима к фишингу (вид интернет-мошенничества, целью которого является получение идентификационных данных пользователей), брутфорс-атакам (систематический перебор всех возможных комбинаций символов до тех пор, пока не будет найдена правильная комбинация) и утечкам данных. С развитием киберугроз и методов взлома данный подход демонстрирует уязвимость [1].

В качестве ответа на такие атаки в государственных приложениях все чаще внедряется многофакторная аутентификация, требующая подтверждения личности через несколько независимых факторов. Технические стандарты (ГОСТ Р 57580.1-2017) [2] определяют три основных категории аутентификационных факторов:

– что-то, что знает пользователь – пароли, PIN-коды, контрольные вопросы;

– что-то, что есть у пользователя – токен, смарт-карта, SMS-код;

– что-то, что является частью пользователя – отпечатки пальцев, сканирование лица, голосовая идентификация.

Основные преимущества МФА:

– защита от наиболее распространенных атак: фишинга, брутфорса;

– поддержка различных сценариев использования (удаленный доступ, мобильные приложения);

– интеграция с PKI-инфраструктурой (инфраструктурой открытых ключей, Public Key Infrastructure) для государственных сервисов;

– совместимость с требованиями GDPR (европейский закон) и ФЗ-152 (Федеральным законом «О персональных данных») о персональных данных.

Основные недостатки МФА:

– увеличение времени аутентификации;

– необходимость наличия дополнительных устройств (телефон, токен);

– возможность перехвата SMS-кодов;

– сложности при восстановлении доступа.

Примеры внедрения МФА:

– Единая система идентификации и аутентификации (ЕСИА) в России использует СМС-коды и электронную подпись;

– Госуслуги поддерживают вход через МФА (пароль + подтверждение по телефону или e-mail).

Биометрическая аутентификация

Биометрическая аутентификация становится ключевым элементом современных систем информационной безопасности, предлагая уникальное сочетание высокой надежности и удобства пользователя [3]. В отличие от традиционных методов, основанных на знаниях (пароли) или владении (токены), биометрия использует уникальные физиологические или поведенческие характеристики человека, что существенно усложняет возможность несанкционированного доступа.

Согласно исследованиям, глобальный рынок биометрических технологий растет со среднегодовым темпом 15,2 % [4], а в государственном секторе их внедрение ускоряется благодаря нормативным требованиям. Например, стандарты NIST SP 800-63B и ISO/IEC 19794 [5] регламентируют использование биометрии в системах идентификации, устанавливая требования к точности (FAR/FRR) и защите данных.

Основные преимущества биометрической аутентификации:

– высокая точность (вероятность ошибки менее 0,01% для современных алгоритмов распознавания лица);

– удобство использования (не требует запоминания паролей или ношения токенов);

– неотторгаемость (биометрические характеристики сложно передать третьим лицам).

Однако, внедрение биометрии сопряжено с рядом технических и правовых вызовов, таких как:

– угрозы спуфинга (использование масок, фотографий или синтезированных голосов [6]);

– проблемы конфиденциальности (хранение и обработка биометрических шаблонов);

– нормативные ограничения (требования ФЗ-152 «О персональных данных» [7]).

Примеры внедрения:

– интеграция с Единой системой идентификации и аутентификации (ЕСИА);

– система «Мир Pay» с биометрией;

– биометрический контроль в аэропортах;

– Госуслуги с биометрией;

– банковский сектор (Сбербанк: вход в СберБанк Онлайн по лицу; ВТБ: биометрические банкоматы; Тинькофф: голосовая идентификация в колл-центре).

Заключение

Исходя из всего вышеперечисленного можно сделать вывод, что современные методы аутентификации и авторизации в государственных приложениях демонстрирует сложную эволюцию систем информационной безопасности – от традиционных парольных механизмов к комплексным многофакторным решениям, интегрирующим биометрические, криптографические и аппаратные технологии. Российская практика внедрения этих систем отражает глобальные тренды цифровой трансформации государственных сервисов, одновременно формируя уникальную модель безопасности.

МФА стала отраслевым стандартом, доказав эффективность комбинации «знание+владение+биометрия». Российские решения, такие как ЕСИА, Единая биометрическая система (ЕБС [8]) соответствуют мировым практикам. Достигнуто снижение атак на 80-90 % по сравнению с парольными системами

Биометрические технологии перешли в стадию зрелого внедрения. Сформирована нормативная база (ФЗ-476, стандарты Центрального Банка РФ). Создана масштабируемая инфраструктура (ЕБС с более 15 млн пользователей).

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Десятов С. В. Сравнительный анализ достоинств и недостатков наиболее распространенных методов идентификации и аутентификации пользователей и других участников идентификационных процессов / С. В. Десятов // Интерэкспо Гео-Сибирь. – 2021. – Т. 8. – С. 314-323.
2. Электронный фонд правовых и нормативно-технических документов, Базовый состав организационных и технических мер. [Электронный ресурс]. – Режим доступа: https://docs.cntd.ru/document/1200146534 (дата обращения 10.04.2025).
3. Козлов М. А. Биометрические системы, применяемые для контроля доступа в организациях / М. А. Козлов, А. Н. Поликанин // Интерэкспо Гео-Сибирь. – 2023. – Т. 6, № 1. – С. 111-117.
4. Tadviser, Биометрическая идентификация (мировой рынок). [Электронный ресурс]. – Режим доступа: https://www.tadviser.ru/a/117554 (дата обращения 10.04.2025).
5. Электронный фонд правовых и нормативно-технических документов, Форматы обмена биометрическими данными. [Электронный ресурс]. – Режим доступа: https://docs.cntd.ru/document/1200129505 (дата обращения 10.04.2025).
6. Голос становится объектом права. Как его защитить в эпоху дипфейков и искусственного интеллекта // Tadviser: Государство. Бизнес. Технологии. 2024. [Электронный ресурс]. URL: https://www.tadviser.ru/a/845638 (дата обращения: 10.04.2025 г.)
7. Федеральный закон Российской Федерации от 27 июля 2006 г. № 152 "О персональных данных" (с изменениями на 8 августа 2024 года). URL: https://docs.cntd.ru/document/901990046 (дата обращения: 10.04.2025 г.).
8. Единая биометрическая система (ЕБС) // Tadviser: Государство. Бизнес. Технологии. 2023. [Электронный ресурс]. URL: https://www.tadviser.ru/a/399126/ (дата обращения: 10.04.2025 г.).