

Кондратьев Роман Демьянович
старший преподаватель
кафедры специальных информационных технологий УНК ИТ
Московский университет МВД России имени В.Я. Кикотя
Москва, Россия

Роль многофакторной аутентификации в защите служебной информации МВД России

Аннотация. В статье рассмотрены вопросы применения многофакторной аутентификации (МФА) как ключевого элемента системы защиты служебной информации в органах внутренних дел Российской Федерации. Проведён анализ нормативных, технологических и организационных основ внедрения МФА в автоматизированных информационных системах МВД. Особое внимание уделено интеграции с платформами ЕСИА и ЕБС, использованию биометрических и криптографических методов, а также практическим возможностям реализации поведенческой аутентификации, в том числе на основе клавиатурного почерка. Обоснована необходимость многоуровневой защиты информации в условиях удалённого доступа и высокой степени цифровизации ведомственной деятельности. Выделены преимущества МФА по сравнению с однофакторными моделями, а также обозначены направления дальнейшего развития в контексте повышения защищённости информации и устойчивости к внутренним и внешним угрозам.

Ключевые слова: многофакторная аутентификация, МВД России, информационная безопасность, биометрия, ЕСИА, ЕБС, служебная информация, защита данных, доступ, поведенческая идентификация.

Kondratyev Roman Dem'yanovich
Senior Lecturer
Department of Special Information Technologies of the IT University
Moscow University of the Ministry of Internal Affairs of Russia named after V. Ya. Kikot
Moscow, Russia

The role of multifactor authentication in the protection of official information of the Ministry of Internal Affairs of Russia

Abstract. The article discusses the use of multifactor authentication (MFA) as a key element of the official information protection system in the internal affairs bodies of the Russian Federation. The paper analyzes the regulatory, technological and organizational foundations for the implementation of MFA in the automated information systems of the Ministry of Internal Affairs. Particular attention is paid to integration with the ESIA and EBS platforms, the use of biometric and cryptographic methods, as well as practical opportunities for implementing behavioral authentication, including keyboard handwriting. The necessity of multi-level information protection in the context of remote access and a high degree of digitalization of departmental activities is substantiated. The advantages of MFA over single-factor models are highlighted, as well as directions for further development in the context of improving data security and resilience to internal and external threats.

Keywords: multifactor authentication, Ministry of Internal Affairs, information security, biometrics, ESIA, EBS, official information, data protection, access, behavioral identification.

Информационная безопасность в системе органов внутренних дел Российской Федерации приобретает критически важное значение в условиях стремительного роста киберугроз и цифровизации ведомственных процессов. Хранение, обработка и передача конфиденциальной служебной информации сопряжены с рисками несанкционированного доступа, что требует от МВД применения комплексных и адаптивных методов защиты. Одной из центральных задач в этом контексте становится надёжная проверка подлинности субъектов доступа к автоматизированным системам, базам данных и цифровым сервисам ведомства.

Сложившаяся практика традиционной авторизации — на основе логина и пароля — продемонстрировала свою уязвимость перед методами социальной инженерии, фишинга, программ-вирусов и перебора паролей. Однофакторная аутентификация уже не способна обеспечить достаточный уровень защиты, особенно при удалённом доступе сотрудников к служебным системам, что активно применяется в рамках цифровой трансформации МВД. В этих условиях потребность в более устойчивых решениях ведёт к переходу к многофакторной аутентификации (МФА) как к технологически и методологически оправданному инструменту повышения защищённости служебной информации.

МФА опирается на комбинацию различных факторов подтверждения личности — от знаний и устройств до биометрических характеристик и контекстных признаков поведения. Такая модель затрудняет подделку цифровой идентичности и снижает вероятность компрометации учётных данных. Современные системы МФА применимы не только для внутреннего контурного доступа, но и для реализации межведомственных взаимодействий, что актуализирует разработку единых подходов в рамках государственной цифровой инфраструктуры.

Особое внимание в рамках правоохранительной деятельности привлекают технологии биометрической аутентификации и интеграция с федеральными платформами — Единой системой идентификации и аутентификации (ЕСИА) и Единой биометрической системой (ЕБС). Использование этих решений открывает перспективы перехода к безбумажному удостоверению личности в служебной среде, где оперативность доступа сочетается с соблюдением юридически значимых процедур.

Целью настоящего исследования является всесторонний анализ роли многофакторной аутентификации в обеспечении защиты служебной информации МВД России. Особое внимание будет уделено технологическим механизмам реализации МФА, их нормативному обоснованию, а также специфике внедрения в структуре автоматизированных информационных систем внутренних дел.

Основной фактор, определяющий актуальность внедрения многофакторной аутентификации в органах внутренних дел, заключается в растущей угрозе компрометации служебной информации, циркулирующей в автоматизированных системах. Ключевые сегменты оперативно-служебной деятельности МВД, включая базы розыска, дактилоскопические учёты, криминалистические и статистические реестры, функционируют в условиях цифрового взаимодействия между подразделениями. Нарушение целостности или несанкционированный доступ к этим системам создаёт угрозу не только информационной безопасности, но и легитимности управленческих и следственных решений [1].

Традиционные способы идентификации, основанные на логине и пароле, демонстрируют крайне низкую устойчивость к целевым атакам. Распространение вирусостилеров, использование программ перебора, фишинговых рассылок и утечек из сторонних ресурсов создают условия, при которых однофакторная авторизация становится недопустимой в служебных средах. Статистические данные, собранные по результатам анализа инцидентов в 2022 году, показывают, что до 46% всех атак были нацелены на получение учётных данных, преимущественно через уязвимости аутентификации [3].

Введение многофакторной аутентификации направлено на устранение ключевого недостатка — зависимости от одного типа подтверждения. МФА реализуется через

комбинирование факторов знаний, владения и биометрических характеристик. При этом обеспечивается принцип независимости компонентов: компрометация одного фактора не даёт возможности доступа без второго или третьего. На практике чаще всего используется комбинация пароля с одноразовым кодом, генерируемым токеном или мобильным приложением, либо проверка на основе биометрических признаков. Биометрическая составляющая — лицо, отпечаток пальца, голос или рисунок вен — особенно ценна при работе с удалённым доступом, где физическое удостоверение невозможно [3].

В системе МВД России технологическое применение МФА напрямую связано с инфраструктурой ЕСИА и ЕБС. Эти государственные платформы уже используются для доступа к ведомственным системам, а в перспективе будут дополнены мобильными идентификаторами и электронными паспортами с биометрическими носителями. Переход к этим технологиям закреплён на нормативном уровне, в частности, в постановлении Правительства РФ № 977 и ФЗ № 479-ФЗ, что позволяет встраивать механизмы МФА в юридически значимые процессы, включая получение допусков, удостоверение личности, доступ к базам данных и проведение служебных проверок [5].

Одним из ключевых направлений внедрения многофакторной аутентификации в системе МВД выступает использование биометрических методов. Помимо широко применяемых решений, таких как распознавание отпечатков пальцев и лица, активно развиваются альтернативные подходы. Особое внимание привлекает технология клавиатурного почерка, основанная на анализе индивидуальных особенностей набора текста — временных параметров удержания клавиш, интервалов между нажатиями, ритмики и устойчивых поведенческих паттернов. Эта форма биометрии обладает высоким уровнем стойкости к подделке, так как не может быть скопирована визуально или голосом. Её реализация возможна без специализированного оборудования, что обеспечивает экономическую эффективность по сравнению с другими методами. В контексте ведомственного применения клавиатурная биометрия способна интегрироваться в существующую инфраструктуру служебных рабочих мест. Преимущества данного подхода на фоне других форм аутентификации представлены в таблице 1. [2]

Таблица 1.

Сравнительная таблица методов аутентификации: однофакторная, двухфакторная, многофакторная.

Метод аутентификации	Устойчивость к атакам	Применимость	Стоимость внедрения
Однофакторная	Низкая	Ограниченные или устаревшие системы	Низкая
Двухфакторная	Средняя	Широко используется в коммерческих и ведомственных системах	Средняя
Многофакторная	Высокая	Критически важные системы, государственные и силовые структуры	Средняя–высокая

Анализ внедрённых решений показывает, что современные автоматизированные системы МВД обладают необходимым техническим потенциалом для поддержки многофакторной аутентификации. Большинство персональных устройств сотрудников (служебные смартфоны, планшеты, ноутбуки) оснащены базовыми модулями — сканерами отпечатков пальцев, микрофонами и фронтальными камерами. Эти элементы уже используются для выполнения служебных задач, что позволяет интегрировать МФА без дополнительных затрат на оборудование [5].

Вопросы нормативной и методической поддержки также находят своё решение. Существуют утверждённые регламенты, включающие правила доступа к программно-техническому комплексу ИБД-Ф, оценку полноты дактилоскопических и розыскных учётов, а также алгоритмы контроля использования специализированного портала ГИАЦ

МВД. Всё это делает возможным организацию защищённого доступа на основе МФА, с мониторингом активности и автоматическим выявлением отклонений [4].

Дополнительным направлением развития МФА в МВД является применение криптографической биометрии — использование биометрических шаблонов как компонентов криптографических ключей. Такой подход обеспечивает не только аутентификацию, но и шифрование служебной информации с привязкой к конкретному пользователю. Решения на базе «bioscrypt» позволяют хранить ключи внутри биометрических данных, делая невозможным их извлечение без предъявления оригинала шаблона. Этот метод уже тестируется в ряде ведомств, а его применение в МВД может быть оправдано в наиболее чувствительных сегментах — при доступе к закрытым базам, служебной переписке и материалам оперативной работы [3].

Несмотря на технологические успехи, уровень защищённости информационных систем остаётся зависимым от человеческого фактора. Нарушения регламента, небрежность при обращении с персональными устройствами, несанкционированная передача кодов и паролей — всё это требует параллельной реализации организационных мер. К их числу относятся обязательное обучение сотрудников, внедрение технической блокировки сессий при отклонении от поведенческой модели и автоматическая проверка логов доступа. Вопросы повышения цифровой грамотности становятся частью общего курса информационной безопасности МВД, что находит отражение в ведомственных методиках контроля и в системе оценки результатов служебной деятельности [1].

Внедрение многофакторной аутентификации в МВД России отражает не просто адаптацию к технологическим трендам, а системную трансформацию подходов к обеспечению конфиденциальности, целостности и доступности ведомственных данных. Технический потенциал, нормативная база и положительный опыт позволяют говорить о сформированной инфраструктуре, готовой к масштабному применению МФА в служебных процессах.

Многофакторная аутентификация в условиях цифровой трансформации МВД России перестала быть вспомогательным техническим решением и выступает в роли системного элемента защиты служебной информации. Обоснованность её применения подтверждается необходимостью обеспечения устойчивости к целенаправленным кибератакам, угрозам компрометации учётных данных и несанкционированного доступа к ведомственным информационным ресурсам.

Применение МФА в автоматизированных системах МВД реализуется в сочетании с государственными инфраструктурами ЕСИА и ЕБС, что обеспечивает нормативную легитимность процедуры аутентификации. Интеграция с биометрическими и криптографическими технологиями позволяет адаптировать уровень защиты к классу информации и типу доступа. При этом используются как классические методы (пароли и токены), так и поведенческие механизмы, в том числе клавиатурный почерк.

Технические средства, необходимые для поддержки многофакторной аутентификации, уже присутствуют в устройствах, находящихся на вооружении МВД. Это делает возможным внедрение без значительных финансовых затрат. Методологическая база, включая регламенты контроля доступа и алгоритмы оценки защищённости, позволяет формализовать применение МФА в повседневной оперативно-служебной деятельности.

Для повышения эффективности использования МФА требуется последовательная работа по минимизации влияния человеческого фактора. Это включает формирование пользовательской дисциплины, технический аудит, настройку поведенческого мониторинга и интеграцию аналитических механизмов в существующие платформы.

Переход к многофакторной аутентификации представляет собой логичную и необходимую меру в обеспечении информационной безопасности МВД России. Развитие этих решений должно опираться не только на технологические возможности, но и на институциональную готовность к масштабному применению принципов цифровой идентичности в правоохранительной сфере.

Список источников

1. Бацких, А. В. К вопросу использования новой информационной технологии, связанной с дополнительной аутентификацией субъектов доступа по клавиатурному почерку, в системах защиты информации от несанкционированного доступа на объектах информатизации органов внутренних дел / А. В. Бацких, И. Г. Дровникова, Е. А. Rogozin // Вестник Воронежского института МВД России. – 2020. – № 2. – С. 21-33. – EDN DDVYPU.
2. Крупина, М. А. Цифровизация ведомственного контроля Информационного обеспечения деятельности органов внутренних дел Российской Федерации / М. А. Крупина // Вестник Санкт-Петербургского университета МВД России. – 2023. – № 2(98). – С. 62-70. – DOI 10.35750/2071-8284-2023-2-62-70. – EDN ISDSVR.
3. Надейкина В. С., Лагуткина Т. В. АНАЛИЗ СПОСОБОВ РЕАЛИЗАЦИИ СИСТЕМЫ МНОГОФАКТОРНОЙ АУТЕНТИФИКАЦИИ // Научный результат. Информационные технологии. 2022. №4.
4. Серпилина, Е. К. Особенности обеспечения защиты информации в автоматизированных системах органов внутренних дел / Е. К. Серпилина // Общественная безопасность, законность и правопорядок в III тысячелетии. – 2023. – № 9-2. – С. 306-310. – EDN CPLGHD.
5. Степаненко, Д. А. К вопросу об использовании механизма удаленной идентификации и аутентификации в правоохранительной деятельности / Д. А. Степаненко, А. А. Рудых // Технологии XXI века в юриспруденции: Материалы Третьей международной научно-практической конференции, Екатеринбург, 21 мая 2021 года / Отв. редактор Д.В. Бахтеев. – Екатеринбург: Федеральное государственное бюджетное образовательное учреждение высшего образования "Уральский государственный юридический университет", 2021. – С. 318-326. – EDN GPAAUU.