УДК 004.056.53

МНОГОФАКТОРНАЯ АУТЕНТИФИКАЦИЯ (MFA) КАК БАЗОВЫЙ МЕТОД ЗАЩИТЫ КОРПОРАТИВНОЙ СЕТИ

Жуков Н.А., студент гр.568403

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

Чепикова В.В. – старший преподаватель.

Аннотация. В работе представлен комплексный анализ многофакторной аутентификации (MFA) как фундаментального элемента безопасности корпоративных сетей. Рассмотрены современные векторы атак, направленные на обход традиционных методов MFA, включая атаки «злоумышленник в середине» (AitM) и «усталость от MFA» (MFA Fatigue). Обоснована необходимость перехода к фишингоустойчивым методам на базе протоколов FIDO2 и WebAuthn. Даны практические рекомендации по интеграции MFA в архитектуру «нулевого доверия» (Zero Trust).

Ключевые слова. Многофакторная аутентификация, MFA, информационная безопасность, корпоративная сеть, Zero Trust, AitM, MFA Fatigue, FIDO2, биометрия.

Введение

В современном цифровом мире защита передаваемых данных и корпоративных ресурсов становится одной из приоритетных задач. Традиционные сетевые экраны (firewalls) и виртуальные частные сети (VPN) долгое время служили основой корпоративной безопасности, создавая защищенный периметр вокруг внутренних ресурсов. Однако в условиях стремительной децентрализации ИТ-инфраструктуры, массовой миграции сервисов в облачные среды и повсеместного перехода на удаленный и гибридный форматы работы традиционная модель безопасности, основанная на защите периметра, окончательно утратила свою эффективность. Сегодня сотрудники получают доступ к конфиденциальной коммерческой информации с различных устройств, включая личные (BYOD), и из неконтролируемых публичных сетей. В этой новой реальности парадигма безопасности сместилась от защиты сети к защите данных и строгой идентификации пользователей. Концепция «нулевого доверия» (Zero Trust Architecture, ZTA) предполагает, что ни одному субъекту или устройству нельзя доверять по умолчанию, независимо от их физического или логического местоположения. В основе этой архитектуры лежит непрерывная проверка личности пользователя, где многофакторная аутентификация (MFA) выступает уже не как дополнительная опция, а как фундаментальный, базовый механизм защиты корпоративного контура [1]. Цель данной работы – провести анализ многофакторной аутентификации как базового метода защиты, рассмотреть уязвимости традиционных подходов перед современными угрозами и определить наиболее эффективные способы внедрения фишингоустойчивых решений в корпоративную среду.

Эволюция угроз и кризис парольной защиты

Исторически сложилось так, что основным методом идентификации пользователей в информационных системах выступала парольная защита. Тем не менее, на сегодняшний день пароли представляют собой наиболее уязвимое звено в архитектуре кибербезопасности. Статистические данные ведущих аналитических агентств показывают, что подавляющее большинство успешных кибератак начинается именно с компрометации учетных данных. Проблема усугубляется человеческим фактором: пользователи склонны применять легко угадываемые пароли или повторно использовать одни и те же комбинации для доступа к различным корпоративным и личным сервисам. Даже при внедрении строгих политик сложности паролей злоумышленники активно применяют методы социальной инженерии, фишинг, атаки полного перебора (brute-force) и подстановку ранее утекших учетных данных (credential stuffing). В связи с этим Национальным институтом стандартов и технологий США (NIST) и Европейским агентством по кибербезопасности (ENISA) в рамках требований директивы NIS2 настоятельно рекомендуется отказ от использования исключительно парольной защиты для доступа к критически важной инфраструктуре [2, 3].

Принципы и классификация факторов MFA

В основе многофакторной аутентификации лежит довольно простой принцип: чтобы подтвердить свою личность, пользователю недостаточно предъявить что-то одно. Нужно предоставить как минимум два независимых доказательства. Смысл такого подхода очевиден – если злоумышленник подсмотрит пароль или каким-то образом украдет токен, система все равно его не пропустит, поскольку у него не окажется второго ключа к учетной записи. На практике все эти доказательства (или факторы) принято делить на три большие группы:

То, что мы держим в голове, или фактор знания. Сюда относятся привычные всем пароли, короткие PIN-коды, а также ответы на контрольные вопросы.

То, что находится у нас в руках – фактор владения. Это может быть как обычный смартфон, на который приходит SMS или где работает генератор кодов (например, приложение TOTP), так и специализированное оборудование вроде аппаратных USB-ключей и смарт-карт.

То, кем мы физически являемся, то есть неотъемлемые свойства человека. Речь идет о биометрии: отпечатках пальцев, геометрии лица или рисунке радужной оболочки глаза [4]. Скопировать или передать кому-то такие данные крайне проблематично. Кроме того, современные корпоративные системы все чаще смотрят не только на то, что вводит пользователь, но и на контекст его действий. Технологии адаптивной аутентификации (Adaptive MFA) умеют анализировать, из какой геопозиции происходит попытка входа, в какое время суток, насколько надежно само устройство и не отличается ли сетевое поведение сотрудника от его привычных паттернов.

Современные векторы атак на системы MFA

Несмотря на то, что внедрение базовой MFA критически повышает уровень защищенности, не все ее методы обеспечивают одинаковую степень защиты от современных изощренных кибератак. Выделяют два основных вектора атак на системы многофакторной аутентификации: Первый вектор – атаки типа «злоумышленник в середине» (Adversary-in-the-Middle, AitM). В данном сценарии атакующий разворачивает прокси-сервер, который перехватывает трафик между жертвой и легитимным сервисом. Жертва переходит по ссылке на поддельный сайт. При вводе логина, пароля и одноразового кода (например, из SMS), прокси-сервер в реальном времени передает эти данные на целевой ресурс. После успешной аутентификации сервис выдает легитимный маркер сеанса (session cookie), который перехватывается злоумышленником. Получив маркер, атакующий обходит защиту MFA. Второй вектор – атака типа «усталость от MFA» (MFA Fatigue или Prompt Bombing). Данная техника применяется, когда в качестве второго фактора используются Push-уведомления. Атакующий, заполучив пароль жертвы, инициирует десятки запросов на авторизацию подряд, обычно в ночное время. Непрерывный поток уведомлений вызывает раздражение у пользователя, который в конечном итоге подтверждает запрос, чтобы прекратить спам.

Сравнительный анализ методов аутентификации

Для выбора оптимального решения необходимо оценивать методы MFA по уровню предоставляемой безопасности, устойчивости к описанным атакам и удобству для конечного пользователя. В таблице 1 представлен сравнительный анализ основных методов.

Таблица 1 – Сравнительный анализ методов многофакторной аутентификации

Метод аутентификации	Уровень безопасности	Защита от фишинга (AitM)	Защита от MFA Fatigue	Удобство пользователя
SMS / Email OTP	Низкий	Нет (перехват)	Да (неприменимо)	Высокое
TOTP	Средний	Нет (перехват)	Да (неприменимо)	Среднее
Push-уведомления	Средне-Высокий	Нет(если без контекста)	Нет	Очень высокое
Аппаратные ключи (FIDO2)	Наивысший	Да (криптографическая привязка)	Да (требует физ. контакта)	Среднее (нужен токен)
Биометрия	Высокий	Да	Да	Высокое

Сравнительный анализ методов аутентификации

Для надежной защиты корпоративной сети от современных угроз организациям необходимо переходить к фишингоустойчивым методам MFA. Наиболее эффективным решением является использование протоколов WebAuthn и FIDO2. Аппаратные ключи безопасности (например, YubiKey) или платформенные аутентификаторы используют криптографию с открытым ключом, которая криптографически привязана к конкретному домену (URL-адресу). Если пользователь попадает на фишинговый сайт, ключ просто не выдаст валидный ответ, что делает атаки AitM технически невозможными

Для успешного внедрения MFA в корпоративную среду рекомендуется:

1 Использовать политики условного доступа (Conditional Access): запрашивать MFA с учетом контекста (необычный IP-адрес, новое устройство, доступ к критичным данным).

2 Ограничить Push-уведомления: внедрить функцию «сопоставления чисел» (Number Matching) для защиты от MFA Fatigue.

3 Защитить привилегированные учетные записи (PAM): администраторы должны в обязательном порядке использовать аппаратные ключи безопасности (FIDO2).

Заключение

Многофакторная аутентификация перестала быть опциональным элементом и перешла в разряд базовых требований безопасности для любой корпоративной сети. Однако полагаться на устаревшие методы, такие как SMS, в условиях изощренных атак больше нельзя. Стратегия безопасности должна строиться на внедрении фишингоустойчивой MFA, грамотном управлении доступом на основе контекста и обучении сотрудников, что в совокупности обеспечивает надежный фундамент архитектуры Zero Trust.

Список использованных источников:

Rose, S. Zero Trust Architecture : NIST Special Publication 800-207 / S. Rose [et al.]. – Gaithersburg : National Institute of Standards and Technology, 2020. – 59 p.

Grassi, P. A. Digital Identity Guidelines: Authentication and Lifecycle Management : NIST Special Publication 800-63B / P. A. Grassi [et al.]. – Gaithersburg : National Institute of Standards and Technology, 2017. – 81 p.

Cybersecurity roles and skills for NIS2 Essential and Important Entities / European Union Agency for Cybersecurity (ENISA). – Athens : ENISA, 2025. – 45 p.

Бритвина, В. В. Сравнительный анализ методов аутентификации: от паролей до биометрии и FIDO2 / В. В. Бритвина, С. А. Бердников // Вестник науки. s– 2025. – Т. 1, № 1. – С. 112-118.

UDC 004.056.53

MULTIFACTOR AUTHENTICATION (MFA) AS A BASIC METHOD OF CORPORATE NETWORK SECURITY

Zhukov N.A.

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

Chepikova V.V. – senior lecturer

Abstract. This paper presents a comprehensive analysis of multi-factor authentication (MFA) as a fundamental element of corporate network security. It examines modern attack vectors aimed at bypassing traditional MFA methods, including man-in-the-middle (AitM) attacks and MFA fatigue. It also substantiates the need to transition to phishing-resistant methods based on the FIDO2 and WebAuthn protocols. Practical recommendations for integrating MFA into a Zero Trust architecture are provided.

Keywords: Multi-factor authentication, MFA, information security, corporate network, Zero Trust, AitM, MFA fatigue, FIDO2, biometrics.