

Студ. К.И. Отчик, А.В. Ярмольчик
Науч. рук. П.П. Урбанович
(Кафедра информационных систем и технологий, БГТУ)

ОСОБЕННОСТИ РЕАЛИЗАЦИИ МЕХАНИЗМОВ МНОГОФАКТОРНОЙ АУТЕНТИФИКАЦИИ В ИС

Многофакторная аутентификация (МФА) – это компонент управления доступом, который требует от пользователей подтверждения своей личности с использованием минимум двух различных факторов проверки, прежде чем получить доступ к какому-либо онлайн-ресурсу.

В докладе анализируются основные особенности использования МФА. МФА использует технологии проверки как минимум из двух разных групп или факторов аутентификации пользователя [1].

Основные виды реализации многофакторной защиты:

– биометрическая – форма аутентификации, которая точно и безопасно аутентифицирует пользователей через их мобильные устройства;

– аппаратные токены – небольшие, простые в использовании устройства, которые владелец несет для авторизации доступа к сетевой службе;

– мобильная – процесс проверки пользователя через это устройство или проверки самого устройства;

– внеполосная – тип аутентификации, требующий вторичного метода проверки через отдельный канал связи (примеры: Код Cronto, отправить уведомление, sms-сообщение или голосовое сообщение, мягкий токен) [2].

ЛИТЕРАТУРА

1. Урбанович, П. П. Компьютерные сети и сетевые технологии: учеб. пособие для студ. технических спец. / П. П. Урбанович, Д. М. Романенко. – Минск: БГТУ, 2022. – 608 с.

2. Что такое многофакторная аутентификация (MFA). [Электронный ресурс]– Режим доступа: <https://www.onespan.com/ru/topics/mnogofaktornaja-autentifikacija/> – Дата доступа: 02.04.2023.