



CYBER READINESS  
INSTITUTE

# Руководство по многофакторной аутентификации

---

**Следуйте этим рекомендациям, чтобы понять и внедрить многофакторную аутентификацию в вашей организации**

Малые и средние предприятия, которые ищут практические способы повышения своей кибербезопасности, должны использовать многофакторную аутентификацию (МФА). По данным [Microsoft](#), 99,9% атак с компрометацией учетных записей можно заблокировать, просто используя МФА. Следующее руководство поможет вам ознакомиться с МФА (также известной как двухфакторная аутентификация «2ФА») и понять, как реализовать эту возможность для повышения кибербезопасности для вас и вашей организации.

## Что такое МФА?

МФА требует от пользователей предоставления более одного доказательства (учетных данных) всякий раз, когда они входят в рабочую учетную запись (например, электронную почту компании, платежную ведомость, данные отдела кадров и т. д.). МФА обычно делится на три категории: **что-то, что знает пользователь** (пароль из 15 символов), **что-то, что есть у пользователя** (отпечаток пальца), или **что-то, что пользователь получает** (код, отправленный на его телефон или адрес электронной почты).

## Почему важна МФА?

Киберпреступники хотят скомпрометировать учетные данные для входа и будут использовать различные методы, в том числе выдавать себя за ваше финансовое учреждение или деловых партнеров, чтобы получить их обманным путем. Однако предоставив сотрудникам возможность использовать МФА, вы защитите вашу бизнес-информацию и их данные.

Использование надежных паролей из 15-ти символов — один из важнейших шагов, однако **МФА предлагает техническое решение, ориентированное на человека**. С МФА пароль сотрудника больше не является единственной линией киберзащиты вашей компании. Хакеры, стремящиеся украсть данные вашей компании, не смогут просто угадать или взломать пароль сотрудника. Вместо этого **МФА защитит ваших сотрудников и вашу компанию от этих атак**.

## Как реализовать МФА?

Внедрение МФА не требует аппаратных изменений компьютеров, мобильных устройств или принтеров. Вместо этого существует множество бесплатных и недорогих программных инструментов, которые пользователи могут загрузить на свои корпоративные и личные устройства. Например, вполне вероятно, что ваш провайдер электронной почты предлагает (и поощряет) МФА. Таким образом, можно просто нажать на параметр в настройках, чтобы включить МФА.

Тем не менее, вам может быть интересно узнать, как лучше внедрить МФА в вашей рабочей силе. Во-первых, **вам следует обновить свои политики и процедуры, включив в них конкретные пояснения ваших ожиданий**. Например, все сотрудники должны использовать МФА в своих корпоративных учетных записях электронной почты. Затем вам следует провести **информационные совещания и тренинги** для сотрудников, на которых вы расскажете о своей политике МФА, ожиданиях и объясните, насколько прост этот процесс для них. Наконец, вам следует **назначить человека в вашей организации, который возьмет на себя ответственность за киберготовность, чтобы помочь сотрудникам устранять неполадки**, когда они начнут использовать МФА.

## Где я могу узнать больше?

Теперь, когда у вас есть общее представление о важности МФА для вашего бизнеса и о том, как ее внедрить, вы можете изучить дополнительные ресурсы и практики киберготовности на сайте **BeCyberReady.com**.

### Об Институте киберготовности

Институт киберготовности — это некоммерческая инициатива, объединяющая лидеров бизнеса из разных секторов и географических регионов для обмена ресурсами и знаниями, которые используются с целью разработки бесплатных инструментов кибербезопасности в малых и средних предприятиях (МСП). Изучите основы хорошей кибербезопасности в нашем стартовом наборе или создайте культуру киберготовности в своей организации с помощью самостоятельной онлайн-программы киберготовности. В наших руководствах по ресурсам для удаленной работы и гибридным рабочим местам вы найдете своевременные советы по решению современных киберпроблем. Чтобы узнать больше, посетите сайт [www.BeCyberReady.com](http://www.BeCyberReady.com).