

Чек-лист кибербезопасности бизнеса

Отметьте галочкой вопросы, на которые можете ответить утвердительно

- ☐ У сотрудников отдельные учетные записи?
- ☐ Доступы бывших сотрудников закрыты?
- ☐ Для важных сервисов включена двухфакторная аутентификация?
- ☐ Для разных систем используются разные пароли?
- ☐ Права сотрудников ограничены рабочими задачами?
- ☐ Программы и сайт регулярно обновляются?
- ☐ На устройствах установлена защита?
- ☐ Гостевая сеть Wi-Fi отделена от рабочей?
- ☐ Критичные данные копируются автоматически?
- ☐ Компания проверяла восстановление из резервной копии?
- ☐ Сотрудники знают признаки фишинга?
- ☐ Есть ответственный за инциденты?
- ☐ Сохранены контакты банка, хостинга и технического специалиста?
- ☐ Компания знает, где хранит персональные данные?
- ☐ У подрядчиков нет лишних и бессрочных доступов?

До 5 ответов «Да». Защита требует срочных базовых мер. Начните с важных аккаунтов, прав доступа и резервных копий.

От 6 до 10 ответов «Да». Основы уже есть, но отдельные слабые места способны привести к инциденту. Составьте план на месяц и назначьте ответственного.

От 11 до 15 ответов «Да». В компании выстроена базовая система. Продолжайте проверять восстановление, обучать сотрудников и пересматривать доступы.