

ЧЕК-ЛИСТ ДЛЯ ИТ-КОМАНДЫ

8 проверок защиты корпоративной сети от киберугроз

Отметьте статус каждого пункта. Если результат неизвестен, назначьте проверку и ответственного.

Контрольный пункт	Да	Нет	?
01. Внешние сервисы и интерфейсы Проверьте, что все доступные из интернета сервисы и административные интерфейсы учтены; ненужный доступ закрыт.	☐	☐	☐
02. Обновления Убедитесь, что критические обновления установлены либо назначены сроки и ответственные за их установку.	☐	☐	☐
03. Многофакторная аутентификация Проверьте, что для административного и удаленного доступа используется MFA там, где она поддерживается.	☐	☐	☐
04. Права доступа Проверьте права пользователей и сервисных учетных записей: избыточные полномочия должны быть исключены.	☐	☐	☐
05. Сегментация сети Убедитесь, что между сетевыми сегментами действуют необходимые правила доступа и нет лишних разрешенных соединений.	☐	☐	☐
06. Мониторинг и журналы Проверьте сбор и регулярный анализ событий безопасности, включая подозрительные входы и изменения конфигураций.	☐	☐	☐
07. Резервное копирование Убедитесь, что резервные копии защищены, а восстановление данных успешно проверено на практике.	☐	☐	☐
08. Реагирование на инциденты Проверьте актуальность плана: ответственные, порядок изоляции систем, восстановления и оповещения определены.	☐	☐	☐

Результат проверки

Пункты со статусом «Нет» или «?» требуют дополнительной проверки и плана корректирующих действий. Приоритет определяйте по риску для бизнеса.

Дата проверки: _____ Ответственный: _____