Срочно.

- Установить и настроить Firewall на сервере. Отключить все неиспользуемые порты.
- Сканировать на наличие вирусов и других угроз сервера при помощи антивирусных утилит (по требованию) не реже 1 раза в месяц.
- Создавать раз в неделю (не реже) зашифрованные резервные копии критически важных данных и хранить на съёмных носителях информации. Можно использовать облачные решения (только без автоматической и постоянной синхронизации данных).
- Создавать раз в неделю (не реже) необходимые резервные копии данных, нужные для работы компании.
- Хранить резервные копии (кроме критически важных) на специально выделенном сервере без доступа в Сеть. Можно использовать облачные решения (только без автоматической и постоянной синхронизации данных).
- Срочно поменять все пароли RDP.
- Использовать сложные пароли для RDP (не менее 8-значных с использованием букв и цифр).
- Настроить контроль и блокировку неудачных попыток входа RDP.
- Сменить порт для RDP.
- Реализовать блокировку подключения по RDP учётным записям с пустым паролем.
- Сменить пароли для учётных записей уволенных сотрудников и отключить неиспользуемые учётные записи.
- Защита для RDP – это сложный пароль, домен + конфиденциальность.
- Используя SRP, разрешить запуск исполняемых файлов на компьютере только из определенных папок. Как более простой вариант, можно настроить запрет запуска исполняемых файлов из пользовательских каталогов. Как в первом так и во втором случае, запретить запуск других потенциально опасных файлов (*.bat,*.vbs, *.js, *.wsh, *.com, *.cmd, *.scr, *.pif, *.wsf, *.jse и т.п), а не только *.exe.
  Особое внимание уделить запрету на запуск исполняемых файлов в папках:
  %LocalAppData%
  %Temp%
  %AppData%
  %UserProfile%
  %WinDir%
  %SystemRoot%
- Создать отдельную сетевую папку для каждого пользователя. Права на запись должны быть только у владельца папки.
- Отказаться от использования ОС Windows XP.
- Регулярно устанавливать последние обновления для ОС и критического софта (браузеры, антивирусы, защитные комплексные программы).
- Не использовать пиратские ОС, комплексные антивирусы, Firewall. Устанавливать и обновлять софт с официальных сайтов.
- По возможности, обновится до ОС Windows 10.
- Отключить WPS на роутерах.

- Если настройки роутера позволяют – необходимо скрыть сеть (отключить транслирование имени SSID). Обязательно использовать для Wi-Fi – WPA-шифрование и VPN. Если роутер не поддерживает такую возможность – заменить на новый. При необходимости раздавать Wi-Fi сторонним посетителям офиса, клиентам – настроить гостевую сеть.
- Использовать 12-значный пароль (не меньше) для Wi-Fi. Вовремя обновлять прошивку с исправлениями безопасности для роутеров.
- Защитить компьютеры сотрудников комплексными антивирусными решениями класса Internet Security.

Высокий приоритет.

- Обеспечить бесперебойное электропитание серверной.
- Использовать сложные пароли (не менее 15 символов прописных и строчных букв с комбинацией цифр) для любых учёток и аккаунтов. Для удобства, использовать менеджеры паролей.
- Настроить режим защиты RDP-сессии.
- Настроить шифрование для RDP (реализовать именно режим RDP FIPS140-1 Encryption).
- Привязать RDP к конкретному адаптеру и порту.
- Включить NLA (Network Level Authentication).
- Настройка ACL для подключения по RDP.
- Произвести оптимизацию скорости RDP.
- Произвести оптимизацию сжатия RDP.
- Произвести оптимизацию соотношения потоков данных в RDP.
- Настроить на сервере аутентификацию через SSH-ключи.
- Сменить порт SSH.
- Использовать PKI и SSL/TLS шифрование.
- Ограничить список IP, с которых возможен доступ к серверу.
- Применить способ запуска компонентов системы в их собственном выделенном пространстве (изолированная среда выполнения).

Средний приоритет.

- Настроить аудит файлов и систему обнаружения вторжений.
- Установить единые комплексные антивирусные средства на сервера и рабочие станции.