Dr.WEB®
с 1992 года

# Правила организации системы ИБ для компании с удаленно работающими сотрудниками

Dr.WEB®
с 1992 года

# Правила организации системы ИБ для компании с удаленно работающими сотрудниками

1. Используйте **сложные** пароли (не менее 8 символов, содержащий буквы разного регистра, цифры и спецсимволы) **для всех учетных записей и сервисов**. Используйте **разные пароли для разных сервисов и учетных записей**.

2. Назначьте и используйте **пароль для антивируса**, отличный от пароля к учетным записям. Даже если хакеры проникнут на ваш компьютер, они не смогут внедрить вредоносное ПО, отключив антивирус.

3. Заблокируйте неиспользуемые учетные записи и отключите ненужные сервисы операционной системы (например, возможность удаленного входа, если вы ей не пользуетесь).

4. Запретите сотрудникам работу с правами администратора компьютера.

5. На всех компьютерах сети — и офисных, и принадлежащих сотрудникам, с которых они заходят в сеть компании — должен быть корпоративный антивирус, настройки которого контролирует администратор сети.

6. С помощью Брандмауэра Dr.Web установите ограничение на удаленное подключение, оставив возможность подключения только с определенных адресов. Если вы используете удаленное подключение, измените стандартный порт для подключения к RDP.

7. Используйте только актуальную версию Dr.Web. При соединении с Интернетом антивирус должен обновляться не реже чем раз в час. Контролируйте успешность обновления вирусных баз.

8. При работе в сети никогда не отключайте компоненты антивируса – и запретите это делать сотрудниками (в антивирусе Dr.Web этот запрет стоит по умолчанию). В частности, никогда нельзя отключать файловый монитор SpIDer Guard и Превентивную защиту Dr.Web.

9. Не злоупотребляйте списком исключений для антивирусной проверки, не включайте в него папки с временными файлами и программами. Прежде чем добавить программу в список исключений, посоветуйтесь с технической поддержкой «Доктор Веб».

10. С помощью Офисного/Родительского контроля включите ограничение доступа к заведомо вредоносным сайтам.

11. Включите службу Автоматического обновления и установите все предложенные обновления. Обновите все используемые программы.

12. Разрешите использование на своем компьютере только известных вам сменных носителей (флешек, букридеров, фотокамер и др.).