





ПРАВИЛА БЕЗОПАСНОСТИ ПРИ АДМИНИСТРИРОВАНИИ САЙТОВ








ПАРОЛЬНАЯ ЗАЩИТА

-  Не записывайте пароли на бумаге или в файле на компьютере.
-  Используйте сложные пароли, включающие буквы разного регистра, цифры и специальные символы (!@#\$%^&*)
-  Не используйте в качестве паролей слова или последовательности цифр или букв, которые легко подобрать (например, password, qwerty, 123456).
-  Регулярно меняйте пароли.







АНТИВИРУСНАЯ БЕЗОПАСНОСТЬ

-  Установите на компьютере или ноутбуке антивирусную программу. Периодически обновляйте антивирус.
-  При подозрении на заражение устройства (подвисание, нетипичная работа, самопроизвольные действия) запустите проверку антивируса.
-  При подключении сторонних устройств (флешек, карт памяти, мобильных телефонов) запускайте их проверку антивирусом.
-  Не запускайте неизвестные файлы, особенно с расширением .exe
-  Не скачивайте сомнительные приложения или приложения на неизвестных сайтах. Проверьте приложение антивирусом.



СИСТЕМА УПРАВЛЕНИЯ САЙТОМ (СУС)

-  Обновляйте до актуальных версий программное обеспечение СУС, которое используется вашим сайтом (например, WordPress, Joomla, Drupal, Bitrix, Plone, Zope).
-  Создавайте разные учётные записи для каждого пользователя СУС.
-  Меняйте стандартные настройки СУС, в т.ч. адрес входа в панель администрирования.
-  Регулярно выполняйте резервное копирование данных сайта.

Подробные инструкции и рекомендации смотрите в разделе «Информационная безопасность» на сайте mininform74.ru