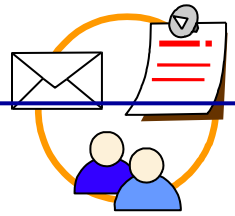
Безопасность работы и конфиденциальность информации в АСУ РСО

Факторы безопасной работы в АСУ РСО

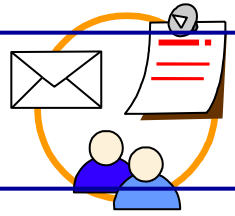
Администратор системы



Права пользователя заданные разработчиками, могут быть изменены администратором системы

Пользователи из числа сотрудников школы могут совмещать несколько ролей

Пользователь в АСУ РСО



Имеет индивидуальное имя и пароль

Имеет доступ к определённым разделам

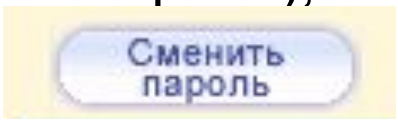
В АСУ РСО обеспечена конфиденциальность информации!!!

Правила корректной работы в системе АСУ РСО

- Не забывать нажимать кнопку «Сохранить» для сохранения введённых данных.
- Помнить о том, что в системе существует ограничение времени работы (ученик–60 мин., все остальные пользователи–15 мин.).
- **Обратить внимание!** Если пользователь не соблюдает время работы в системе, то он будет автоматически «выброшен» из неё без сохранения данных.

Правила безопасной работы в системе АСУ РСО

- Обязательно сменить пароль после первого входа в систему.
- Соблюдать конфиденциальность пароля.
- Не забывать своё **Имя пользователя** и **Пароль (пароль не может быть восстановлен!)**.
- Периодически менять свой пароль - раздел «Персональные настройки» (кнопка Сменить пароль), не менее одного раза в 42 дня.



Политика паролей

Характеристики слабого пароля:

- содержит менее 8 символов;
- слово из словаря;
- повседневно используемое слово;
- компьютерный термин, команда, наименование компаний, web сайтов и т.д;
- день рождения или другая персональная информация;
- регулярные последовательности символов и цифр, например, 111222, abcde, qwerty и т.п.;
- что-либо из вышеперечисленного в обратном написании.

Пример слабого пароля: ABCD1

Характеристики стойкого пароля:

- содержит прописные (A-Z) и строчные буквы (a-z);
- содержит цифры и символы;
- более 8 символов длиной;
- не является словом ни на одном из языков, диалектов, жаргонов, слэнгов;
- не основывается на персональной информации;
- не записан в бумажной или электронной форме.

Пример стойкого пароля: Rh4yi39f8

Запрещенные действия с паролями:

- никому не сообщайте пароль по телефону;
- не указывайте пароль в сообщениях электронной почты;
- не сообщайте пароль вашему руководству (исключение делается для первичного пароля);
- не сообщайте принципы создания пароля (например, "на основе моей фамилии");
- не сообщайте пароль в электронных опросах и незнакомых формах авторизации;
- не сообщайте пароль членам семьи и родственникам;
- не передавайте пароль коллегам на время вашего отпуска.

Сетевой Город ОБРАЗОВАНИЕ

ВНИМАНИЕ!

Если классный руководитель организует выставление текущих оценок силами учебного сектора класса, то не следует сообщать свой пароль учащимся, лучше вести пароль самостоятельно и контролировать работу детей.

Сетевой Город ОБРАЗОВАНИЕ

ВНИМАНИЕ!

Запрещено сообщать пароль кому бы то ни было, включая административный персонал и секретарей. Все пароли являются конфиденциальной информацией.

Общие рекомендации при обработке персональных данных

- На компьютере должна быть включена защищенная паролем заставка, активирующаяся через 10 минут бездействия пользователя.
- При работе в АСУ РСО, экран монитора должен быть скрыт от посторонних глаз.
- Никто из посторонних не должен находится за спиной во время работы с персональными данными в АСУ РСО.
- Не записывайте пароли на бумагу. Не сохраняйте пароли в файлах на каком-либо носителе (например, флэшка, мобильный телефон и т.п.) без шифрования.
- Пароль должен изменяться не менее одного раза в 42 дня, для системных учетных записей раз в три месяца.

Ответственность

Согласно **ст. 24 Федерального закона «О персональных данных»** на лиц, виновных в нарушении его требований, возлагается гражданская, уголовная, административная, дисциплинарная и иная предусмотренная законодательством РФ ответственность.