



УТВЕРЖДАЮ  
Директор МОУ «ЦО №1»  
г. Ясногорска  
Т.М. Елагина

**Инструкция**  
по организации парольной защиты  
в информационных системах муниципального общеобразовательного учреждения  
«Центр образования № 1» г. Ясногорска Тульской области

1. Инструкция по организации парольной защиты в информационных системах муниципального общеобразовательного учреждения «Центр образования № 1» г. Ясногорска Тульской области регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационных системах муниципального общеобразовательного учреждения «Центр образования № 1» г. Ясногорска Тульской области, а также контроль за действиями пользователей при работе с паролями.

2. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей на автоматизированных рабочих местах (далее – АРМ) информационных систем муниципального общеобразовательного учреждения «Центр образования № 1» г. Ясногорска Тульской области и контроль за действиями пользователей при работе с паролями возлагается на ответственного за обеспечение защиты персональных данных в информационных системах муниципального общеобразовательного учреждения «Центр образования № 1» г. Ясногорска Тульской области (далее Ответственный).

3. Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями АРМ самостоятельно с учетом следующих требований:

3.1. Длина пароля должна быть не менее 7 символов;

3.2. В числе символов пароля необходимо использовать буквы в верхнем и/или нижнем регистрах и цифры;

3.3. Пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т. д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т. п.);

3.4. При смене пароля новое значение должно отличаться от предыдущего не менее чем в 3-х позициях;

3.5. Личный пароль пользователь не имеет права сообщать никому.

4. Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

5. В случае если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на Ответственного.

6. Для генерации стойких значений паролей могут применяться специальные программные средства.

7. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в 180 дней.

8. Внеплановая смена личного пароля или удаление (блокирование) учетной записи пользователя в случае прекращения его полномочий (увольнение и т. п.) должна производиться Ответственным немедленно после окончания последнего сеанса работы данного пользователя с системой.

9. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение и другие обстоятельства) Ответственного.

10. В случае компрометации личного пароля пользователя должны быть немедленно предприняты меры в соответствии с п. 8 или п. 9 настоящей инструкции в зависимости от полномочий владельца скомпрометированного пароля.

11. Хранение сотрудником (исполнителем) значений своих паролей на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у Ответственного или руководителя подразделения в опечатанном личной печатью (штампом организации) конверте.



УТВЕРЖДАЮ  
Директор МОУ «ЦО №1»  
г. Ясногорска  
Т.М. Елагина

**ИНСТРУКЦИЯ**  
**по антивирусной защите в информационных системах**  
**муниципального общеобразовательного учреждения**  
**«Центр образования № 1» г. Ясногорска Тульской области**

1. Настоящая инструкция предназначена для ответственного за обеспечение безопасности персональных данных в информационных системах муниципального общеобразовательного учреждения «Центр образования № 1» г. Ясногорска Тульской области (далее – Ответственный, МОУ «ЦО №1» Г. Ясногорска) и пользователей, обрабатывающих персональные данные на автоматизированных рабочих местах (далее АРМ) информационных систем МОУ «ЦО №1» Г. Ясногорска.

2. В целях обеспечения антивирусной защиты на АРМ производится антивирусный контроль.

3. Ответственность за поддержание установленного в настоящей инструкции порядка проведения антивирусного контроля возлагается на ответственного за обеспечение безопасности персональных данных в информационных системах МОУ «ЦО №1» Г. Ясногорска.

4. К применению на АРМ допускаются только лицензионные и сертифицированные ФСТЭК России антивирусные средства.

5. На АРМ запрещается установка программного обеспечения, не связанного с выполнением функций МОУ «ЦО №1» Г. Ясногорска.

6. Пользователи АРМ при работе с носителями информации обязаны перед началом работы осуществить проверку их на предмет отсутствия компьютерных вирусов.

7. Обновление антивирусных баз осуществляется ежедневно путем настройки в антивирусном средстве доступа к серверам обновлений разработчика антивирусного средства. В случае невозможности настроить доступ к серверам обновлений разработчика антивирусного средства, Ответственный один раз в неделю осуществляет установку пакетов обновлений антивирусных баз, осуществляет контроль их подключения к антивирусному программному обеспечению и проверку жесткого диска и съемных носителей на наличие вирусов.

8. При обнаружении компьютерного вируса пользователи обязаны немедленно поставить в известность Ответственного и прекратить какие-либо действия на АРМ.

9. Ответственный проводит расследование факта заражения АРМ компьютерным вирусом. «Лечение» зараженных файлов осуществляется путем выбора соответствующего пункта меню антивирусной программы и после этого вновь проводится антивирусный контроль.

10. В случае обнаружения вируса, не поддающегося лечению, Ответственный обязан удалить инфицированный файл в соответствующую папку антивирусного пакета, и проверить работоспособность АРМ. В случае отказа АРМ – произвести восстановление соответствующего программного обеспечения.

11. Обо всех фактах заражения АРМ, Ответственный обязан ставить в известность ответственного за организацию обработки персональных данных и своего непосредственного руководителя.