ИНСТРУКЦИЯ
ПО ОРГАНИЗАЦИИ ПАРОЛЬНОЙ ЗАЩИТЫ
в информационных системах персональных данных муниципального автономного общеобразовательного учреждения «Гимназия №1 Октябрьского района г. Саратова»

1. Общие положения.

1.1. Настоящая инструкция разработана в соответствии с требованиями:

- Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»;
- постановления Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- приказа ФСТЭК России от 18.02.2013 г. №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке и информационных системах персональных данных»

1.2. С целью ограничения доступа к информационным системам (далее – ИС) устанавливается единая система установки паролей на базе общего и прикладного программного обеспечения средств защиты информации.

1.3. Личные пароли должны выбираться пользователями **самостоятельно**, с учетом следующих требований:

- длина пароля должна быть не менее 6 буквенно-цифровых символов;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования автоматизированного рабочего места и т. д.), а также общепринятые сокращения;
- в пароле должны присутствовать символы трех категорий - прописные, строчные, десятичные цифры;
- запрещается выбирать пароли, которые использовались ранее.

1.4. Правила хранения пароля:

- запрещается записывать пароли на бумаге, в файл, электронной записной книжке и других носителях информации, в том числе на предметах;
- запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

1.5. Личный пароль сотрудника, допущенного к информационным

ресурсам ИС, составляет его секрет и разглашению не подлежит.

1.6. Удаление учетной записи пользователя ИС в случае его увольнения должно производиться немедленно после окончания последнего сеанса работы данного пользователя, по представлению служебной записки сотрудником Администратору.

1.7. Имя пользователя и индивидуальный пароль являются идентификатором пользователя в ИС.

1.8. При авторизации в ИС пользователь обязан ввести свое имя пользователя и набрать индивидуальный пароль, после чего он получает доступ к отведенным для него ресурсам.

1.9. С целью контроля над реализацией прав доступа пользователей к информационным ресурсам ИС должно быть организовано ведение аудита ИС с использованием встроенных механизмов операционной системы и средств защиты информации.

1.10. Действия пользователей, допущенных к информационным ресурсам, хранимым на сервере ИС, могут протоколироваться. Ответственность за уничтожение, изменение информации несет пользователь, под чьим именем операция была зарегистрирована, если в результате расследования не определено конкретное виновное лицо.

1.11. Нарушение пользователями целостности установленного программного обеспечения, а также самовольное установление программ, не предназначенных для выполнения должностных обязанностей, категорически запрещается.

2. Порядок плановой и внеплановой смены личного пароля.

2.1. Плановая смена паролей должна проводиться регулярно, но не реже одного раза в 3 месяца.

2.2. Внеплановая смена любого пароля пользователя ИС производится:

- по просьбе самого пользователя;
- по требованию администратора безопасности ИС.

2.3. В случае временного прекращения полномочий пользователя ИС (болезнь, отпуск, командировка и т. п.) администратором безопасности ИС производиться блокировка учетной записи пользователя по представлению служебной записки руководителем структурного подразделения.

2.4. Внеплановая смена паролей должна производиться в случае

прекращения полномочий (увольнение, переход на другую работу и другие обстоятельства) администраторов безопасности ИС и других сотрудников, которым по роду работы были предоставлены либо полномочия по управлению ИС в целом, либо полномочия по управлению системой защиты информации данной ИС, а значит, кроме личного пароля, им были известны пароли других пользователей.

3. Действия при компрометации пароля.

3.1. В случае компрометации личного пароля хотя бы одного пользователя ИС смена паролей производится в объеме, зависящем от полномочий владельца скомпрометированного пароля.

3.2. По всем фактам компрометации паролей проводят служебное расследование.

3.3. Все пользователи ИС, должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, за разглашение парольной информации и сохранность информации на отведенных ему разделах сервера.

Лист ознакомления
с инструкцией по парольной защите в информационных системах персональных данных муниципального автономного общеобразовательного учреждения
«Гимназия №1 Октябрьского района г. Саратова»

N п/п	Фамилия, имя, отчество	Дата	Занимаемая должность	Подпись
1	2	3	4	5

N п/п	Фамилия, имя, отчество	Дата	Занимаемая должность	Подпись
1	2	3	4	5