РАССМОТРЕНО:	ПРИНЯТО:	УТВЕРЖДАЮ:
Педагогическим советом	Общим собранием	Директор ГБОУ школы № 612
ГБОУ школы №612	работников	Центрального района СПб
Протокол №1 от 30.08.2018.	Протокол №3 от 31.08.2018.	_____Трошнева Е.Н.

Приказ № 212 от 01.09.2018.

Подписано цифровой подписью: ГБОУ школа № 612 Центрального района СПб

ГБОУ школа № 612 Центральног о района СПб

ИНСТРУКЦИЯ
по организации парольной защиты информационной системы обработки персональных данных в ГБОУ школе № 612 Центрального района Санкт-Петербурга

Обозначения и сокращения

АРМ – автоматизированное рабочее место;

ИСПДн – информационная система персональных данных;

ЛВС - локальная вычислительная сеть;

НСД – несанкционированный доступ;

ПДн – персональные данные;

ЭВМ – электронно-вычислительная машина;

СЗИ – средства защиты информации;

СЗПДн – система (подсистема) защиты персональных данных.

I. Общие положения

Данная инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в ИСПДн ГБОУ школа №612 района Санкт-Петербурга (далее школа), а также контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.

1. Организационное обеспечение процессов генерации, смены и прекращения действия паролей в ИСПДн школы возлагается на работника школы, ответственного за информационную безопасность.
2. Личные пароли генерируются и распределяются централизованно для авторизации в ИСПДн школы с учетом следующих требований:
   - длина пароля должна быть не менее 6 символов;
   - в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);
   - пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования рабочих станций и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);

- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях;
- личный пароль пользователь не имеет права сообщать никому.

3. Для входа в операционную систему на рабочих станция состоящих в ИСДн школы должна применяться двухфакторная аутентификация.
4. Владельцы паролей должны быть предупреждены об ответственности за разглашение парольной информации.
5. При наличии в случае возникновении нештатных ситуаций, форс-мажорных обстоятельств и т.п. технологической необходимости использования имен и паролей некоторых работников в их отсутствие, такие работники обязаны сразу же после смены своих паролей их новые значения (вместе с именами соответствующих учетных записей) в запечатанном конверте передавать на хранение работнику школы, ответственному за информационную безопасность школы.
6. Руководитель структурного подразделения школы, в котором работает такой сотрудник, в период его отсутствия по письменному согласованию с директором школы обращается к специалисту по защите информации и получает конверт с именем учетной записи и паролем.
7. После возвращения работника, в отсутствие которого была использована его парольная информация, производится внеплановая смена пароля.
8. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в год.
9. Внеплановая смена личного пароля или блокирование учетной записи пользователя автоматизированной системы в случае прекращения его полномочий (увольнение, переход на другую работу внутри школы, отпуск на срок более 10 дней и т.п.) должна производиться по докладной записке, подаваемой не позднее, чем за 2 рабочих дня до прекращения полномочий пользователя, руководителем структурного подразделения работнику, ответственному за информационную безопасность.
10. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри школы) администраторов средств защиты и других работников, которым по роду работы были предоставлены полномочия по управлению парольной защитой подсистем ИСПДн школы.
11. В случае компрометации личного пароля пользователя автоматизированной системы должны быть немедленно предприняты меры в соответствии с п.5 или п.6 настоящей Инструкции в зависимости от полномочий владельца скомпрометированного пароля.
12. Хранение работником значений своих паролей на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у ответственного за информационную безопасность или руководителя отдела (возможно вместе с персональными ключевыми дискетами и идентификатором TouchMemory).
13. Контроль за соблюдением порядка смены, хранения и использования паролей возлагается на работника школы, ответственного за информационную безопасность.

Лист ознакомления
с Инструкцией

№ п/п	Фамилия, имя, отчество работника	Дата ознакомления с Инструкцией	Подпись работника