Государственное бюджетное общеобразовательное учреждение
средняя общеобразовательная школа № 301
Фрунзенского района Санкт-Петербурга

ПРИНЯТО
Педагогическим Советом
протокол от 30.08.2021 № 1

УТВЕРЖДАЮ
Директор школы_____/Е.С. Спиридонова/
Приказ от 31.08.2021 № 230

ПОЛОЖЕНИЕ

об организации парольной защиты ГБОУ средняя школа № 301 Фрунзенского района Санкт-Петербурга

1. Общие положения

1.1. Положение по организации парольной защиты (далее – Положение) разработано в соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Указом Президента Российской Федерации от 06.03.1997 № 188 (в ред. от 23.09.2005) «Об утверждении перечня сведений конфиденциального характера», постановлением Правительства Российской Федерации от 17 ноября 2007 года № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», постановлением Правительства Российской Федерации от 15 сентября 2008 года №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», иными нормативными правовыми актами Российской Федерации.

1.2. Настоящее Положение регламентирует организационно-техническое обеспечение процессов установки, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационных системах ГБОУ средней школы №301 Фрунзенского района Санкт-Петербурга (далее – Учреждение).

1.3. Положение призвано регламентировать контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.

1.4. Организационное и техническое обеспечение процессов установки, использования, смены и прекращения действия паролей в информационных системах Учреждения и контроль за действиями исполнителей при работе с паролями возлагается заместителя директора по ШИС.

2. Правила формирования паролей

2.1. Пароли доступа первоначально формируются ответственным за информационную безопасность – заместителем директора по ШИС, а в дальнейшем выбираются пользователями самостоятельно, но с учетом требований, изложенных ниже:

2.1.1. Пароль должен состоять не менее чем из шести символов.

2.1.2. В пароле обязательно должны присутствовать буквы из верхнего и нижнего регистров, цифры и специальные символы.

2.1.3. Пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, известные названия, словарные и жаргонные слова и т.д.), последовательности символов и знаков (111, qwerty, abcd и т.д.), общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.), аббревиатуры, клички домашних животных, номера автомобилей, телефонов и другие значимые сочетания букв и знаков, которые можно основываясь на информации о пользователе.

2.1.4. При смене пароля новый пароль должен отличаться от старого не менее чем в двух позициях.

2.2. Пароли служебных и привилегированных учетных записей информационных систем регистрируются в журнале, форма которого установлена в *приложении 1.* Страницы журнала регистрации паролей нумеруются, прошиваются и скрепляются печатью и подписью руководителя ОУ. Журнал регистрации паролей храниться в сейфе. К служебным учетным записям относятся учетные записи администратора, используемые для управления работой информационных систем. К привилегированным учетным записям относятся учетные записи Руководства учреждения.

3. Ввод пароля

3.1. При вводе пароля пользователю необходимо исключить произнесение его вслух, возможность его подсматривания посторонними лицами и техническими средствами (стационарными и встроенными в мобильные телефоны видеокамерами и т.п.).

4. Порядок смены личных паролей

4.1. Смена паролей проводится регулярно, перед началом новой учебной четверти.

4.2. В случае прекращения полномочий пользователя (увольнение, переход на другую работу и т.п.) ответственный за информационную безопасность – заместитель директора по ШИС должен немедленно удалить его учетную запись сразу после окончания последнего сеанса работы данного пользователя с системой.

4.3. Срочная (внеплановая) полная смена паролей производится в случае компроментации пароля пользователя или прекращения полномочий (увольнение, переход на другую работу и т.п.) других работников, которым по роду работы были предоставлены полномочия по управлению системой парольной защиты.

4.4. Смена пароля производится самостоятельно каждым пользователем в соответствии с пунктом 2.1 настоящей Инструкции.

4.5. Временный пароль, заданный ответственным за информационную безопасность – заместителем директора по ШИС, при регистрации нового пользователя, следует изменить при первом входе в систему.

5. Хранение паролей

5.1. Хранение пользователем своего пароля на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе либо в сейфе руководителя Учреждением.

5.2. Запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации.

5.3. Запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

6. Действия в случае утери и компрометации пароля

6.1. В случае утери или компрометации пароля пользователя должны быть немедленно приняты меры в соответствии с пунктом 4.3 или пунктом 4.4 настоящей Инструкции в зависимости от полномочий владельца скомпрометированного пароля.

7. Ответственность при организации парольной защиты

7.1. Пользователи Учреждения несут персональную ответственность за несоблюдение требований по парольной защите.

7.2. Пользователи Учреждения должны быть ознакомлены с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение информации о пароле.

7.3. Ответственность за организацию парольной защиты в Учреждении возлагается на ответственного за информационную безопасность заместителя директора по ШИС.

7.4. Пользователи за несоблюдение или нарушение парольной защиты несут ответственность в соответствии с действующим законодательством Российской Федерации.

Приложение 1

Форма журнала регистрации паролей пользователей

Журнал
регистрации паролей пользователей

№ п/п	Фамилия, имя, отчество	Имя пользователя	Пароль (6 символов)	Срок действия пароля	
				Дата выдачи	Дата окончания действия