Томская область
городской округ
закрытое административно-территориальное образование Северск
АДМИНИСТРАЦИЯ ЗАТО СЕВЕРСК

УПРАВЛЕНИЕ МОЛОДЕЖНОЙ И СЕМЕЙНОЙ ПОЛИТИКИ, ФИЗИЧЕСКОЙ КУЛЬТУРЫ И СПОРТА
(УМСП ФКиС Администрации ЗАТО Северск)

ПРИКАЗ

№ 245

31.07.2025

Об утверждении инструкции по организации парольной защиты в Управлении молодежной и семейной политики, физической культуры и спорта Администрации ЗАТО Северск

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»

ПРИКАЗЫВАЮ:

1. Утвердить прилагаемую инструкцию по организации парольной защиты в Управлении молодежной и семейной политики, физической культуры и спорта Администрации ЗАТО Северск (далее – УМСП ФКиС Администрации ЗАТО Северск, Управление).
2. Разместить приказ на официальном сайте УМСП ФКиС Администрации ЗАТО Северск в информационно-телекоммуникационной сети «Интернет» (https://умсп.зато-северск.рф/).
3. Старшему инспектору УМСП ФКиС Администрации ЗАТО Северск Ковалёвой К.Ю. ознакомить заинтересованных лиц в настоящим приказом.
4. Контроль за исполнением настоящего приказа оставляю за собой.

Врио начальника Управления Т.Н. Малыщенко

Приложение
к приказу УМСП ФКиС
Администрации ЗАТО Северск
от «31» июля 2025 года № 245

УТВЕРЖДЕНА

приказом
УМСП ФКиС
Администрации ЗАТО
Северск
от 31.07.2025 № 245

ИНСТРУКЦИЯ
по организации парольной защиты
в Управлении культуры Администрации ЗАТО Северск

I. ОБЩИЕ ПОЛОЖЕНИЯ

1. Инструкция по организации парольной защиты в Управлении молодежной и семейной политики, физической культуры и спорта Администрации ЗАТО Северск (далее соответственно - Управление, Инструкция) регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационной системе персональных данных (далее – ИСПДн) Управление, а также контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.

2. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех системах, подсистемах ИСПДн и контроль за действиями обслуживающего персонала систем при работе с паролями возлагаются на ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных, назначенного приказом начальника Управление (далее - Ответственный за обеспечение безопасности персональных данных).

II. ПРАВИЛА ФОРМИРОВАНИЯ ПАРОЛЕЙ

3. Личные пароли пользователей должны соответствовать следующим требованиям:

1) длина пароля должна быть не менее 8 символов;

2) в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (!, @, #);

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

4) при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях;

5) личный пароль пользователь не имеет права сообщать никому. В случае если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на ответственного за обеспечение безопасности персональных данных.

III. ВВОД ПАРОЛЯ

4. При вводе пароля пользователю необходимо исключить произнесение его вслух, возможность его подсматривания посторонними лицами (человек за спиной, наблюдение человеком за движением пальцев в прямой видимости или в отраженном свете) и техническими средствами (стационарными и встроенными в мобильные телефоны видеокамерами).

IV. ПОРЯДОК ВЫДАЧИ И СМЕНЫ ЛИЧНЫХ ПАРОЛЕЙ

5. Генерацию паролей и выдачу их пользователям выполняет Ответственный за обеспечение безопасности персональных данных.

6. Смена паролей должна проводиться регулярно, но не реже одного раза в год.

7. В случае прекращения полномочий пользователя (увольнения, перехода на другую работу), Ответственный за обеспечение безопасности персональных данных должен немедленно выполнить удаление его учётной записи сразу после окончания последнего сеанса работы данного пользователя с системой.

8. Срочная (внеплановая) полная смена паролей должна производиться в случае прекращения полномочий (увольнения, перехода на другую работу) Ответственного за обеспечение безопасности персональных данных, которым по роду работы были предоставлены полномочия по управлению системой парольной защиты.

9. Смена пароля производится самостоятельно каждым пользователем в соответствии с пунктом 2 Инструкции и/или в соответствии с указанием в системном баннере-предупреждении (при наличии технической возможности).

10. Пароль, заданный Ответственным за обеспечение безопасности персональных данных при регистрации нового пользователя, может быть заменен пользователем системы в соответствии с правилами пунктов 3 и 6 настоящей инструкции.

V. ХРАНЕНИЕ ПАРОЛЯ

11. Запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах.

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

13. Хранение пользователем своего пароля на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у ответственного за обеспечение безопасности персональных данных.

VI. ДЕЙСТВИЯ В СЛУЧАЕ УТЕРИ ИЛИ КОМПРОМЕТАЦИИ ПАРОЛЯ

14. В случае утери или компрометации пароля пользователя должны быть немедленно предприняты следующие меры:

1) владелец скомпрометированного пароля должен сообщить о факте утери или компрометации пароля Ответственному за обеспечение безопасности персональных данных;

2) владелец скомпрометированного пароля должен немедленно произвести смену скомпрометированного пароля.

VII. ОТВЕТСТВЕННОСТЬ ПРИ ОРГАНИЗАЦИИ ПАРОЛЬНОЙ ЗАЩИТЫ

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

16. Ответственность за организацию парольной защиты в Управлении и контроль исполнения настоящей инструкции возлагается на Ответственного за обеспечение безопасности персональных данных.