Приложение № 5
Приложение к приказу руководителя комитета физической культуры и спорта администрации города Ставрополя

от «28» 12 2018 г. № 265-ОД

П О Р Я Д О К

ПАРОЛЬНОЙ ЗАЩИТЫ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ КОМИТЕТА ФИЗИЧЕСКОЙ КУЛЬТУРЫ И СПОРТА АДМИНИСТРАЦИИ ГОРОДА СТАВРОПОЛЯ

г. Ставрополь
2018 г.

СПИСОК СОКРАЩЕНИЙ

РМ	Автоматизированное рабочее место
СПДн	Информационная система персональных данных
ВС	Локально-вычислительная сеть
Дн	Персональные данные
ЭВМ	Персональная электронная вычислительная машина
ВТ	Средства вычислительной техники
ИО	Фамилия имя отчество

СОДЕРЖАНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Порядок парольной защиты (далее – Порядок) включает в себя взаимоувязанный комплекс организационно-технических мер, регламентирующих генерацию и/или выбор, использование, хранение, уничтожение парольной информации в информационных системах персональных данных комитета физической культуры и спорта администрации города Ставрополя (далее - Комитет).

1.2. Требования настоящего Порядка являются неотъемлемой частью комплекса мер безопасности и защиты информации в Комитете.

1.3. Требования настоящего Порядка распространяются на всех должностных лиц и сотрудников подразделений Комитета, использующих в работе ИСПДн, а также всех видов программного обеспечения (ПО), эксплуатируемого в Комитете.

1.4. Ознакомление сотрудников Комитета с требованиями Порядка проводит Администратор безопасности ИСПДн под роспись в журнале или на самом документе.

1.5. В целях закрепления знаний по вопросам практического исполнения требований Порядка, разъяснения возникающих вопросов, проводятся (при необходимости) персональные инструктажи пользователей ИСПДн Комитета.

1.6. В случае невозможности исполнения требований настоящего Порядка в полном объеме, например:

– в нештатных ситуациях, возникающих вследствие отказов, сбоев, ошибок, стихийных бедствий, побочных влияний;

– злоумышленных действий.

Практическая «глубина» исполнения настоящего Порядка определяется Администратором безопасности ИСПДн по согласованию с ответственным по защите ПДн Комитета.

2. ФУНКЦИИ СОТРУДНИКОВ

1.1. Непосредственное исполнение, организация и контроль исполнения требований настоящего Порядка в Комитете осуществляется всеми пользователями ИСПДн, а именно:

– Пользователь ИСПДн:

- регулярная (с частотой, установленной настоящим Порядком) смена используемой в работе парольной информации;
- выбор парольной информации с качеством, установленным настоящим Порядком;

– Администратор безопасности ИСПДн:

- организационно-методическое обеспечение процессов генерации, смены и удаления паролей в ИСПДн Комитета;
- разработка всех необходимых инструкций по вопросам парольной защиты ИСПДн Комитета;
- организация доведения до пользователей ИСПДн Комитета требований по парольной защите;
- организация периодического и выборочного контроля исполнения сотрудниками Комитета требований настоящего Порядка;
- согласование выдачи управляющих учетных записей к ИСПДн;

- текущий контроль действий персонала Комитета по работе с паролями (автоматизированный контроль качества паролей – при наличии программно-технических средств);
- техническое обеспечение (при наличии программно-технических средств) процессов генерации/выбора, смены и удаления паролей, соответствующая конфигурация ИСПДн.

3. КАЧЕСТВО И ОБРАЩЕНИЕ ПАРОЛЬНОЙ ИНФОРМАЦИИ

3.1. Пароли доступа к аппаратно-программным вычислительным средствам, информационным ресурсам Организации формируются (выбираются) пользователями этих ресурсов с учетом следующих требований к качеству парольной информации:

№ п/п	Параметр качества пароля	Администратор	Пользовател
1.	Минимальная длина пароля в символах	10	8[1]
2.	Максимальная длина пароля в символах	32	16
3.	Содержание в пароле букв верхнего и нижнего регистра	да	да
4.	Содержание в пароле специальных символов (@, #, $, &, * и т.п.) и цифр	обязательно	рекомендуетс я
5.	Содержание в пароле личных имен, фамилий, кличек домашних животных, № телефонов, дат рождения, географических названий, именований АРМ и т.п.	нет	нет
6.	Содержание в пароле общепринятых сокращений (ПЭВМ, ЛВС, USER, SYSOP и т.д.)	нет	нет
7.	Минимальное отличие нового пароля от предыдущего (в позициях)	3	3
8.	Максимальный срок действия пароля	30 дней	60 дней
9.	Минимальный срок действия пароля	нет	нет
10.	Дополнительный (типа TM, eToken[2] или другие электронные ключи) идентификатор	рекомендуется	рекомендуетс я
11.	Пароль на заставку монитора	да	да

[1] При использовании электронных ключей (USB, Touch Memory) не менее 6 символов.

[2] При использовании электронного ключа такого типа требования вышеприведенной таблицы актуальны только по пунктам №1 и №9.

3.2. Хранение сотрудником (администратором, пользователем) личных паролей допускается только в личном сейфе (запираемом шкафу, ящике), либо в сейфе (запираемом шкафу, ящике) администратора, либо в сейфе (запираемом шкафу, ящике) руководителя отдела. При этом бумажный носитель должен быть упакован в отдельный опечатанный конверт.

3.3. Личные пароли и/или дополнительные идентификаторы (электронные ключи) пользователи и администраторы самостоятельно никому не имеют права сообщать и(или) передавать[3];

3.4. Внеплановая смена/удаление пароля (и при возможности учетной записи) пользователя или администратора автоматизированной системы Комитета в случае прекращения его полномочий должна производиться немедленно после окончания последнего сеанса работы данного пользователя с системой.

3.5. Внеплановая полная смена паролей должна производиться в случае прекращения полномочий Администратора безопасности ИСПДн, других сотрудников, которым по роду работы были предоставлены либо полномочия по управлению ИСПДн, либо полномочия по управлению подсистемой защиты информации ИСПДн[4].

3.6. В случае компрометации пароля доступа в ИСПДн Администратором безопасности ИСПДн должны быть немедленно предприняты меры в зависимости от полномочий владельца скомпрометированного пароля и обстоятельств компрометации.

3.7. Все сотрудники Комитета обязаны по первому требованию Администратора безопасности ИСПДн предъявить значения действующего личного пароля для контроля соответствия установленным требованиям, а после проверки провести немедленную его смену.

3.8. Администратор безопасности ИСПДн, по согласованию с ответственным за обеспечение безопасности ПДн проводит ежеквартальный выборочный контроль выполнения сотрудниками Комитета требований Порядка с отметками в отдельном журнале. О фактах несоответствия качества паролей и/или условий обеспечения их сохранности Администратор ИСПДн докладывает ответственному за обеспечение безопасности ПДн.

4. ОБРАЩЕНИЕ ДОПОЛНИТЕЛЬНЫХ ИДЕНТИФИКАТОРОВ

4.1. В целях усиления процедур идентификации и аутентификации в ИСПДн Комитета, пользователи ИСПДн могут использовать дополнительные индивидуальные электронные идентификаторы (смарт-карты, eToken и т.д.) совместно с личным паролем доступа.

---

[3] Сотрудники Комитета раскрывают значение своего пароля и/или передают физический идентификатор только своим непосредственным руководителям в случае производственной необходимости и/или при проведении контрольно-проверочных мероприятий. По окончанию производственных и/или контрольно-проверочных работ сотрудники производят немедленную смену значений раскрытых паролей

[4] Смена паролей производится для учетных записей систем, в которых не используется аутентификация посредством дополнительных идентификаторов (Touch Memory, eToken и т.п.)

4.2. Дополнительные идентификаторы выдаются и учитываются в соответствии с «Инструкцией по внесению изменений в списки пользователей и наделению их полномочиями доступа к ресурсам информационных систем персональных данных»:

– сотрудники получают дополнительные идентификаторы под роспись;

– Администратор безопасности ИСПДн, по обращению к нему сотрудников, регистрирует дополнительные идентификаторы в ИСПДн Комитета и инструктирует сотрудников с учетом требований настоящего порядка и правил эксплуатации для дополнительных идентификаторов.

4.3. Сотрудники Комитета, получившие в пользование дополнительные идентификаторы, лично обеспечивают надежное круглосуточное безопасное хранение и использование идентификаторов. Оставление идентификатора без присмотра запрещается.

4.4. В случае утери дополнительного идентификатора сотрудники немедленно ставят об этом в известность Администратора безопасности ИСПДн и своего непосредственного руководителя. Администратор организуют немедленную блокировку утерянных ключей в автоматизированных системах.

5. ПЕРЕСМОТР ПОРЯДКА

5.1. Порядок подлежит полному пересмотру в случае приобретения Комитетом новых (дополнительных к имеющимся штатным) автоматизированных средств управления парольной защитой и(или) генерации/выбора паролей.

5.2. В остальных случаях Порядок подлежит частичному пересмотру.

5.3. Полный пересмотр данного Порядка проводится с целью проверки соответствия определенных данным документом мер защиты реальным условиям применения их в ИСПДн Управления.

5.4. Изменения в Порядке (сведения о них) фиксируется в листе регистрации изменений (Приложение 1).

5.5. Вносимые изменения не должны противоречить другим положениям Порядка. При получении изменений к данному Порядку, руководители отделов Комитета в течение трех рабочих дней вносят свои предложения и/или замечания к поступившим изменениям.

6. ОТВЕТСТВЕННЫЕ ЗА ОРГАНИЗАЦИЮ И КОНТРОЛЬ ВЫПОЛНЕНИЯ ПОРЯДКА

6.1. Ответственность за соблюдение требований настоящего Порядка возлагается на всех сотрудников Комитета.

6.2. Ответственность за организацию контрольных и проверочных мероприятий по вопросам парольной защиты возлагается на Администратора безопасности ИСПДн.

6.3. Ответственность за общий контроль информационной безопасности возлагается на ответственного за обеспечение безопасности ПДн Комитета.

ПРИЛОЖЕНИЕ 1. ФОРМА РЕГИСТРАЦИИ ИЗМЕНЕНИЙ В ИНСТРУКЦИИ

ЛИСТ № _____ регистрации изменений в Порядке

№ п.п.	Дата	Внесенное изменение	Основание (наименование, № и дата документа)	Кем внесено изменение (должность, подпись)

Лист ознакомления
с «Порядком парольной защиты в информационных системах персональных данных Комитета физической культуры и спорта администрации города Ставрополя»

№ п/п	Фамилия, инициалы сотрудника	Дата ознакомления	Расписка сотрудника в ознакомлении