УТВЕРЖДАЮ
Руководитель комитета культуры и молодежной политики
администрации города Ставрополя
_____ / Н.П. Головин
«_9_» _января_ 2023 г.
М.П.

ПОРЯДОК
парольной защиты в информационных системах персональных данных
комитета культуры и молодежной политики
администрации города Ставрополя

г. Ставрополь
2023 г.

Содержание

1. Используемые сокращения

АИБ ИСПДн	–	Администратор информационной безопасности ИСПДн
АРМ	–	автоматизированное рабочее место
ИС	–	информационная система
ИСПДн	–	информационная система персональных данных
КЗ	–	контролируемая зона
НСД	–	несанкционированный доступ
ОС	–	операционная система
ПДн	–	персональные данные
ПО	–	программное обеспечение
ППО	–	прикладное программное обеспечение
ПЭВМ	–	персональная электронно-вычислительная машина
СВТ	–	средства вычислительной техники
СЗИ	–	система защиты информации
СЗПДн	–	система защиты персональных данных
СКЗИ	–	средства криптографической защиты информации
СПО	–	системное программное обеспечение
ССОП	–	сеть связи общего пользования
СУБД	–	система управления базами данных
ТС	–	технические средства

2. Общие положения

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 культуры и молодежной политики администрации города Ставрополя (далее – комитет).

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

Требования настоящего Порядка распространяются на всех пользователей ИСПДн комитета, использующих все виды программного обеспечения, эксплуатируемого в комитете.

Ознакомление с требованиями Порядка пользователей ИСПДн осуществляет администратор информационной безопасности ИСПДн под роспись в «Журнале учета проведения инструктажей по вопросам защиты информации» или на нем самом. Лист ознакомления с Порядком представлен в Приложении 2.

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

3. Функции сотрудников

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;

АИБ 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.

4. Качество и обращение парольной информации

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

п.п.	Параметр качества пароля	Администратор	Пользова
	Минимальная длина пароля в символах	10	8[1]
	Максимальная длина пароля в символах	32	16
	Содержание в пароле букв верхнего и нижнего регистра	да	да
	Содержание в пароле специальных символов (@, #, $, &, * и т.п.) и цифр	обязательно	рекоменд
	Содержание в пароле личных имен, фамилий, кличек домашних животных, № телефонов, дат рождения, географических названий, именований АРМ и т.п.	нет	нет
	Содержание в пароле общепринятых сокращений (ПЭВМ, ЛВС, USER, SYSOP и т.д.)	нет	нет

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

п.п.	Параметр качества пароля	Администратор	Пользова
	Минимальное отличие нового пароля от предыдущего (в позициях)	3	3
	Максимальный срок действия пароля	30 дней	60 дне
	Минимальный срок действия пароля	нет	нет
	Дополнительный (типа ТМ, eToken[2] или другие электронные ключи) идентификатор	рекомендуется	рекоменд
	Пароль на заставку монитора	да	да

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) начальника отдела. При этом бумажный носитель должен быть упакован в отдельный опечатанный конверт.

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

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

Внеплановая полная смена паролей должна производиться в случае прекращения полномочий АИБ ИСПДн, другими сотрудниками, которым по роду работы были предоставлены либо полномочия по управлению ИСПДн, либо полномочия по управлению подсистемой защиты информации ИСПДн[4].

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

---

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

[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.)

АИБ ИСПДн, по согласованию с Ответственным за обеспечение безопасности и обработки ПДн комитета и при его непосредственном участии, проводит ежеквартальный выборочный контроль выполнения сотрудниками комитета требований Порядка с отметками в «Плане внутренних проверок состояния защиты персональных данных». О фактах несоответствия качества паролей и/или условий обеспечения их сохранности АИБ ИСПДн докладывает Ответственному за обеспечение безопасности и обработки ПДн.

5. Обращение дополнительных идентификаторов

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

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 подпись;
- АИБ 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.

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

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

6. Порядок пересмотра документа

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

В остальных случаях Порядок подлежит частичному пересмотру.

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

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

Вносимые изменения не должны противоречить другим положениям Порядка. При получении изменений к данному Порядку, начальники отделов комитета в течение 3 (трех) рабочих дней вносят свои предложения и/или замечания к поступившим изменениям.

7. Ответственные за организацию и контроль выполнения порядка

Ответственность за соблюдение требований настоящего Порядка возлагается на всех сотрудников комитета, участвующих в обработке ПДн.

Ответственность за организацию контрольных и проверочных мероприятий по вопросам парольной защиты возлагается на АИБ ИСПДн.

Ответственность за общий контроль информационной безопасности возлагается на Ответственного за обеспечение безопасности и обработку ПДн комитета.

Приложение 1 – Лист регистрации изменений

Лист регистрации изменений в инструкции

№ п/п	Внесенное изменение	Основание (наименование, номер и дата документа)	Лицо, внесшее изменения		Дата внесения изменения
			Фамилия, инициалы	Подпись	

Приложение 2 – Лист ознакомления

Лист ознакомления

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

УТВЕРЖДАЮ
Руководитель комитета культуры и молодежной политики
администрации города Ставрополя
_____/ Н.П. Головин
«___» _____ 2021 г.
М.П.

ПОРЯДОК
парольной защиты в информационных системах персональных данных
комитета культуры и молодежной политики
администрации города Ставрополя

г. Ставрополь
2021 г.

Содержание

1. Используемые сокращения

АИБ ИСПДн	–	Администратор информационной безопасности ИСПДн
АРМ	–	автоматизированное рабочее место
ИС	–	информационная система
ИСПДн	–	информационная система персональных данных
КЗ	–	контролируемая зона
НСД	–	несанкционированный доступ
ОС	–	операционная система
ПДн	–	персональные данные
ПО	–	программное обеспечение
ППО	–	прикладное программное обеспечение
ПЭВМ	–	персональная электронно-вычислительная машина
СВТ	–	средства вычислительной техники
СЗИ	–	система защиты информации
СЗПДн	–	система защиты персональных данных
СКЗИ	–	средства криптографической защиты информации
СПО	–	системное программное обеспечение
ССОП	–	сеть связи общего пользования
СУБД	–	система управления базами данных
ТС	–	технические средства

2. Общие положения

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 культуры и молодежной политики администрации города Ставрополя (далее – комитет).

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

Требования настоящего Порядка распространяются на всех пользователей ИСПДн комитета, использующих все виды программного обеспечения, эксплуатируемого в комитете.

Ознакомление с требованиями Порядка пользователей ИСПДн осуществляет администратор информационной безопасности ИСПДн под роспись в «Журнале учета проведения инструктажей по вопросам защиты информации» или на нем самом. Лист ознакомления с Порядком представлен в Приложении 2.

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

3. Функции сотрудников

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;

– АИБ 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.

4. Качество и обращение парольной информации

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

№ п.п.	Параметр качества пароля	Администратор	Пользователь
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	рекомендуется
5.	Содержание в пароле личных имен, фамилий, кличек домашних животных, № телефонов, дат рождения, географических названий, именований АРМ и т.п.	нет	нет

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

№ п.п.	Параметр качества пароля	Администратор	Пользователь
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 ТМ, eToken[2] или другие электронные ключи) идентификатор	рекомендуется	рекомендуется
11.	Пароль на заставку монитора	да	да

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) начальника отдела. При этом бумажный носитель должен быть упакован в отдельный опечатанный конверт.

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

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

Внеплановая полная смена паролей должна производиться в случае прекращения полномочий АИБ ИСПДн, другими сотрудниками, которым по роду работы были предоставлены либо полномочия по управлению ИСПДн, либо полномочия по управлению подсистемой защиты информации ИСПДн[4].

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

[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.)

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

АИБ ИСПДн, по согласованию с Ответственным за обеспечение безопасности и обработки ПДн комитета и при его непосредственном участии, проводит ежеквартальный выборочный контроль выполнения сотрудниками комитета требований Порядка с отметками в «Плане внутренних проверок состояния защиты персональных данных». О фактах несоответствия качества паролей и/или условий обеспечения их сохранности АИБ ИСПДн докладывает Ответственному за обеспечение безопасности и обработки ПДн.

5. Обращение дополнительных идентификаторов

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

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 подпись;

– АИБ 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.

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

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

6. Порядок пересмотра документа

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

В остальных случаях Порядок подлежит частичному пересмотру.

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

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

Вносимые изменения не должны противоречить другим положениям Порядка. При получении изменений к данному Порядку, начальники отделов комитета в течение 3 (трех) рабочих дней вносят свои предложения и/или замечания к поступившим изменениям.

7. Ответственные за организацию и контроль выполнения порядка

Ответственность за соблюдение требований настоящего Порядка возлагается на всех сотрудников комитета, участвующих в обработке ПДн.

Ответственность за организацию контрольных и проверочных мероприятий по вопросам парольной защиты возлагается на АИБ ИСПДн.

Ответственность за общий контроль информационной безопасности возлагается на Ответственного за обеспечение безопасности и обработку ПДн комитета.

Приложение 1 – Лист регистрации изменений

Лист регистрации изменений в инструкции

№ п/п	Внесенное изменение	Основание (наименование, номер и дата документа)	Лицо, внесшее изменения		Дата внесения изменения
			Фамилия, инициалы	Подпись	

Приложение 2 – Лист ознакомления

Лист ознакомления

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