Приложение № 8

к распоряжению главы

городского округа Истра

от 18.08.2021 № 251-Р

**Инструкция**

**по организации парольной защиты**

**в сегменте «Истра-2» государственной информационной системы «Единая информационная система оказания государственных и муниципальных услуг Московской области»**

**1. Общие положения**

* 1. Данная инструкция по организации парольной защиты в сегменте «Истра-2» государственной информационной системы «Единая информационная система оказания государственных и муниципальных услуг Московской области» администрации городского округа Истра (далее – Сегмент ЕИСОУ) регламентирует процессы генерации, смены и прекращения действия паролей (удаления учётных записей пользователей) в Сегменте ЕИСОУ, а также контроль над действиями пользователей и обслуживающего персонала информационных систем при работе с паролями.
  2. Осуществление процессов генерации, использования, смены и прекращения действия паролей в Сегменте ЕИСОУ и контроль за действиями исполнителей и обслуживающего персонала информационной системы при работе с паролями возлагается на администратора информационной безопасности информационных систем и информационных систем персональных данных (далее – администратор безопасности информационных систем) Сегмента ЕИСОУ.

1. Термины и определения
   1. **Информация** - сведения (сообщения, данные) независимо от формы их представления *(ст. 2 ФЗ РФ от 27.07.2006 г. N 149-ФЗ «Об информации, информационных технологиях и защите информации»).*
   2. **Персональные данные** - любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных) (*ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).*
   3. **Пароль** - секретная комбинация цифр, знаков, слов, или осмысленное предложение, служащие для защиты информации от несанкционированного доступа к информационным ресурсам.
   4. **Компрометация пароля** – раскрытие, обнаружение или утеря пароля.
2. Правила формирования паролей
   1. Личные пароли должны генерироваться и распределяться централизованно.
   2. Ответственность за правильность формирования и распределения паролей в Сегменте ЕИСОУ возлагается на администратора безопасности Сегмента ЕИСОУ.
   3. Ответственность за правильность формирования и распределения паролей для доступа на автоматизированные рабочие места гражданских служащих Сегмента ЕИСОУ возлагается на системного администратора Сегмента ЕИСОУ.
   4. При ручном назначении пароля он должен соответствовать следующим параметрам:
   5. Длина пароля должна быть не менее 6 символов.
   6. Пароль не должен включать в себя слова, которые содержатся в словарях (русских или иностранных), имена, фамилии и отчества людей, клички животных, имена вымышленных персонажей, различные географические наименования, даты рождения, номера телефонов и другую личную информацию.
   7. При смене пароля новое значение должно отличаться от предыдущего не менее чем в 5 позициях.
3. Порядок смены личных паролей
   1. Смена паролей доступа в Сегмент ЕИСОУ должна проводиться регулярно, не реже одного раза в 120 дней, централизованно, администратором безопасности Сегмента ГИС МО «Единая информационная система управления государственной и муниципальной службой МО».
   2. Смена паролей доступа на автоматизированные рабочие места гражданских служащих Сегмента ЕИСОУ должна проводиться регулярно, не реже одного раза в 120 дней, централизованно, системным администратором Сегмента ЕИСОУ.
   3. В случае прекращения полномочий пользователя (увольнение, переход на другую работу и т.п.) должно производиться немедленное удаление его учетных записей доступа в Сегмент ЕИСОУ, а также учетные данные для доступа на автоматизированное рабочее место.
   4. Срочная (внеплановая) полная смена паролей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и т.п.) ответственного за защиту персональных данных, администратора безопасности информационных систем и других государственных гражданских служащих, которым по роду работы были предоставлены полномочия по управлению системой парольной защиты.
4. Хранение пароля.
   1. Запрещается входить в Сегмент ЕИСОУ под учетной записью и паролем другого пользователя.
5. Действия в случае утери и компрометации пароля.
   1. В случае подозрения в компрометации пароля пользователя должна быть немедленно проведена внеплановая процедура смены пароля.
   2. По факту компрометации пароля может быть проведено служебное расследование.
6. Ответственность при организации парольной защиты.
   1. Каждый пользователь Сегмента ЕИСОУ несет персональную ответственность за соблюдение требований настоящей Инструкции и за все действия, совершенные от имени его учетной записи в Сегменте ЕИСОУ, если с его стороны не было предпринято необходимых действий для предотвращения компрометации пароля его учетной записи.
   2. Ответственность за контроль проведения мероприятий по организации парольной защиты в Сегменте ЕИСОУ возлагается на администратора безопасности Сегмента ЕИСОУ.
   3. За разглашение информации ограниченного доступа и нарушение порядка работы в Сегменте ЕИСОУ, обрабатывающем информацию ограниченного доступа, государственные гражданские служащие могут быть привлечены к гражданской, уголовной, административной, дисциплинарной и иной предусмотренной законодательством Российской Федерации ответственности.