

**Муниципальное казенное общеобразовательное учреждение  
Кукаринская основная школа**

СОГЛАСОВАНО педагогическим советом Протокол от 28.02.2022 № 5	УТВЕРЖДАЮ Директор: _____ О.А. Астраханцева Приказ от 02.03.2022 № 19.
---------------------------------------------------------------------	---------------------------------------------------------------------------------

**Положение  
по организации парольной защиты**

**1 Общие положения**

Настоящая инструкция устанавливает основные правила введения парольной защиты информационной системы персональных данных в МКОУ Кукаринской основной школе Лежневского района Ивановской области (далее – Учреждение). Положение регламентирует организационно-техническое обеспечение генерации, смены и прекращения действия паролей в информационной системы персональных данных, а также контроль за действиями пользователей системы при работе с паролями. Настоящее Положение оперирует следующими основными понятиями:

- **Идентификация** - присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.
- **ИСПДн** – информационная система персональных данных.
- **Компрометация**- факт доступа постороннего лица к защищаемой информации, а также подозрение на него.
- **Объект доступа** - единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа.
- **Пароль** – уникальный признак субъекта доступа, который является его (субъекта) секретом.
- **Правила доступа** - совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.
- **Субъект доступа** - лицо или процесс, действия которого регламентируются правилами разграничения доступа.
- **Несанкционированный доступ** - доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или АС.

**2 Правила генерации паролей**

- 2.1 Персональные пароли должны генерироваться специальными программными средствами административной службы.
- 2.2 Длина пароля должна быть не менее 8 символов.
- 2.3 В составе пароля должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы.

- **компрометация**- факт доступа постороннего лица к защищаемой информации, а также подозрение на него.
- **Объект доступа** - единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа.
- **Пароль** – уникальный признак субъекта доступа, который является его (субъекта) секретом.
- **Правила доступа** - совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.
- **Субъект доступа** - лицо или процесс, действия которого регламентируются правилами разграничения доступа.
- **Несанкционированный доступ** - доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или АС.

## 1 Правила генерации паролей

- 1.1 Персональные пароли должны генерироваться специальными программными средствами административной службы.
- 1.2 Длина пароля должна быть не менее 8 символов.
- 1.3 В составе пароля должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы.
- 1.4 Пароль не должен включать в себя:
  - легко вычисляемые сочетания символов;
  - клавиатурные последовательности символов и знаков;
  - общепринятые сокращения;
  - аббревиатуры;
  - номера телефонов, автомобилей;
  - прочие сочетания букв и знаков, ассоциируемые с пользователем;
  - при смене пароля новое сочетание символов должно отличаться от предыдущего не менее чем на 2 символа.

1.5 Допускается использование единого пароля для доступа субъекта доступа к различным информационным ресурсам одной ИСПДн объекта образования.

## **2 Порядок смены паролей**

2.1 Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в месяц.

2.2 Полная внеплановая смена паролей всех пользователей должна производиться в случае прекращения полномочий администраторов средств защиты или других сотрудников, которым по роду службы были предоставлены полномочия по управлению парольной защитой.

2.3 Полная внеплановая смена паролей должна производиться в случае компрометации личного пароля одного из администраторов ИСПДн.

2.4 В случае компрометации личного пароля пользователя надлежит немедленно ограничить доступ к информации с данной учетной записи, до момента вступления в силу новой учетной записи пользователя или пароля.

## **3 Обязанности пользователей при работе с парольной защитой**

3.1 При работе с парольной защитой пользователям запрещается:

- разглашать кому-либо персональный пароль и прочие идентифицирующие сведения;
- предоставлять доступ от своей учетной записи к информации, хранящейся в ИСПДн посторонним лицам;
- записывать пароли на бумаге, файле, электронных и прочих носителях информации, в том числе и на предметах.

3.2 Хранение пользователем своего пароля на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе.

3.3 При вводе пароля пользователь обязан исключить возможность его перехвата сторонними лицами и техническими средствами.

## **4 Случаи компрометации паролей**

4.1 Под компрометацией следует понимать:

- физическая утеря носителя с информацией;
- передача идентификационной информации по открытым каналам связи;
- проникновение постороннего лица в помещение физического хранения носителя парольной информации или алгоритма или подозрение на него (срабатывание сигнализации, повреждение устройств контроля НСД (слепков печатей), повреждение замков и т. п.);

- визуальный осмотр носителя идентификационной информации посторонним лицом;
- перехват пароля при распределении идентификаторов;
- сознательная передача информации постороннему лицу.

#### 4.2 Действия при компрометации пароля:

- скомпрометированный пароль сразу же выводится из действия, взамен его вводятся запасной или новый пароль;
- о компрометации немедленно оповещаются все участники обмена информацией. Пароль вносится в специальные списки, содержащие скомпрометированные пароли и учетные записи.

### **5 Ответственность пользователей при работе с парольной защитой**

- 5.1 Повседневный контроль за действиями сотрудников школы при работе с паролями, соблюдением порядка их смены, хранения и использования, возлагается на ответственного за систему защиты информации в информационной системе персональных данных.
- 5.2 Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.
- 5.3 Ответственность за организацию парольной защиты возлагается на ответственного за систему защиты информации в информационной системе персональных данных.
- 5.4 Ответственность в случае несвоевременного уведомлении ответственного за систему защиты информации в информационной системе персональных данных о случаях утери, кражи, взлома или компрометации паролей возлагается на владельца взломанной учетной записи.



