УТВЕРЖДАЮ
министр цифрового развития
и связи Кузбасса
_____ М.В. Садиков
«17» марта 2020 г.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ
органам местного самоуправления и подведомственным учреждениям по организации идентификации и аутентификации субъектов доступа и объектов доступа в информационной системе персональных данных

I. Общие положения

1. Настоящие Правила регламентируют порядок и процедуры присвоения субъектам и объектам доступа уникального признака (идентификатора), сравнения предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверки принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности), а также организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационной системе персональных данных (далее - ИСПДн) органа местного самоуправления Кемеровской области – Кузбасса (далее – ОМСУ) и контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.

II. Идентификация и аутентификация пользователей, являющихся внутренними пользователями

2. При доступе в информационную систему персональных данных (далее - ИСПДн) осуществляется идентификация и аутентификация пользователей, являющихся сотрудниками ОМСУ (внутренних пользователей), и процессов, запускаемых от имени этих пользователей, а также процессов, запускаемых от имени системных учетных записей. К внутренним пользователям относятся следующие должностные лица ОМСУ:

1) администратор ИСПДн;

2) администратор информационной безопасности (далее - ИБ) ИСПДн;

3) администратор резервного копирования;

4) ответственные сотрудники, выполняющие при эксплуатации ИСПДн свои должностные обязанности (функции) в соответствии с должностными регламентами (инструкциями), утвержденными в министерстве и которым в ИСПДн присвоены учетные записи;

5) администратор виртуальной инфраструктуры (ВИ).

В качестве внутренних пользователей дополнительно рассматриваются должностные лица обладателя информации, заказчика, уполномоченного лица и (или) оператора иной информационной системы, а также лица, привлекаемые на договорной основе для обеспечения функционирования ИСПДн (ремонт, гарантийное обслуживание, регламентные и иные работы) в соответствии с организационно-распорядительными документами. Для каждого внутреннего пользователя в ИСПДн должны быть заведены учетные записи.

3. Пользователи ИСПДн однозначно идентифицируются и аутентифицируются для всех видов доступа, кроме тех видов доступа, которые определяются как действия, разрешенные до идентификации и аутентификации в соответствии с Положением об управлении доступом субъектов доступа к объектам доступа в ИСПДн.

4. Аутентификация пользователя в ИСПДн осуществляется с использованием паролей. Также на усмотрение администратора ИБ ИСПДн могут применяться аппаратные средства в случае многофакторной (двухфакторной) аутентификации.

5. В ИСПДн обеспечивается возможность однозначного сопоставления идентификатора пользователя с запускаемыми от его имени процессами.

III. Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов

6. В ИСПДн устанавливаются и реализуются следующие функции управления идентификаторами пользователей и устройств:

1) формирование идентификатора, который однозначно идентифицирует пользователя и (или) устройство;

2) присвоение идентификатора пользователю и (или) устройству;

3) предотвращение повторного использования идентификатора пользователя и (или) устройства в течение одного года;

4) блокирование идентификатора пользователя после 90 дней неиспользования;

5) в качестве ответственного за создание, присвоение и уничтожение идентификаторов пользователей и устройств определен Администратор ИБ ИСПДн.

IV. Управление средствами аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации

7. В ИСПДн устанавливаются и реализуются следующие функции управления средствами аутентификации (аутентификационной информацией) пользователей:

1) изменение аутентификационной информации (средств аутентификации), заданной их производителями и (или) используемой при внедрении системы защиты ИСПДн;

2) выдача средств аутентификации пользователям;

3) генерация и выдача начальной аутентификационной информации (начальных значений средств аутентификации);

4) установление характеристик пароля: длина пароля не менее шести символов, алфавит пароля не менее 6 символов, максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки - 5 попыток, блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации от 15 минут, смена паролей не более чем через 120 дней;

5) блокирование (прекращение действия) и замена утерянных, скомпрометированных или поврежденных средств аутентификации;

6) назначение необходимых характеристик средств аутентификации (в том числе механизма пароля);

7) обновление аутентификационной информации (замена средств аутентификации) с периодичностью не более чем через 120 дней;

8) защита аутентификационной информации от неправомерных доступа к ней и модифицирования.

8. В случае компрометации личного пароля пользователя ИСПДн должны быть немедленно предприняты меры в зависимости от полномочий владельца скомпрометированного пароля:

1) внеплановая смена личного пароля или удаление учетной записи пользователя ИСПДн в случае прекращения его полномочий (увольнение, переход на другую работу внутри организации и т.п.) должна производиться Администратором ИБ ИСПДн немедленно после окончания последнего сеанса работы данного пользователя с системой;

2) внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри организации и другие обстоятельства) Администратора ИБ ИСПДн и других сотрудников, которым по роду работы были предоставлены полномочия по управлению парольной защитой ИСПДн.

9. В качестве ответственного за хранение, выдачу, инициализацию, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации устройств определен Администратор ИБ ИСПДн.

V. Защита обратной связи при вводе аутентификационной информации

10. В ИСПДн осуществляется защита аутентификационной информации в процессе ее ввода для аутентификации от возможного использования лицами, не имеющими на это полномочий.

11. Защита обратной связи "система - субъект доступа" в процессе аутентификации обеспечивается исключением отображения для пользователя действительного значения аутентификационной информации и (или) количества вводимых пользователем символов аутентификационной информации. Вводимые символы пароля могут отображаться условными знаками "*", "•" или иными знаками.

VI. Ответственность при организации идентификации и аутентификации

12. Ответственность за реализацию правил идентификации и аутентификации субъектов доступа и объектов доступа в соответствии с требованиями настоящих Правил возлагается на Администратора ИБ ИСПДн.

13. Ответственность за поддержание установленного порядка и соблюдение требований настоящих Правил возлагается на Администратора ИБ ИСПДн и пользователей ИСПДн.

14. Периодический контроль за выполнением всех требований настоящих Правил осуществляется комиссией по проведению мероприятий по защите персональных данных.

Начальник отдела данных
и информационной безопасности  С.С. Фомин