КОМИТЕТ
ЦИФРОВОГО РАЗВИТИЯ
ЛЕНИНГРАДСКОЙ ОБЛАСТИ

ПРИКАЗ

от 20 августа 2020 года № 15

Об утверждении Правил генерации и смены паролей при использовании государственных информационных систем, информационных систем персональных данных и объектов критической информационной инфраструктуры Ленинградской области

В соответствии с пунктами 2.11, 2.1.2, 2.13 Положения о Комитете цифрового развития Ленинградской области, утвержденного постановлением Правительства Ленинградской области 05.08.2019 № 364, п. АНЗ.5 Приложения № 2 Требований к защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 № 17, пункта АНЗ.5 Приложения к Составу и содержанию организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденных приказом ФСТЭК России от 18.02.2013 № 21

п р и к а з ы в а ю

1. Утвердить Правила генерации и смены паролей при использовании государственных информационных систем, информационных систем персональных данных и объектов критической информационной инфраструктуры Ленинградской области, согласно приложению.

2. Контроль за исполнением настоящего приказа возложить на первого заместителя председателя Комитета цифрового развития Ленинградской области – начальника департамента информационной безопасности и инфраструктуры.

Председатель
Комитета цифрового развития
Ленинградской области В.А. Кузнецова

УТВЕРЖДЕНЫ
приказом Комитета
цифрового развития
Ленинградской области
от 20 августа 2020 № 15
(Приложение)

Правила генерации и смены паролей при использовании государственных информационных систем, информационных систем персональных данных и объектов критической информационной инфраструктуры Ленинградской области

1. Общие положения

1.1 Настоящие правила устанавливают порядок и правила генерации, использования паролей в программных средствах информационной безопасности и самих государственных информационных системах ограниченного доступа, информационных системах персональных данных и объектах критической информационной инфраструктуры Ленинградской области

1.2 Правила распространяются на всех пользователей и администраторов.

2. Требования к паролям

2.1 Пароли не должны основываться на каком-либо одном слове, выданном идентификаторе, имени, кличке, паспортных данных, номерах страховок и т.д.

2.2 Пароли не должны основываться на типовых шаблонах и идущих подряд на клавиатуре или в алфавите символов, например, таких, как: qwerty, 1234567, abcdefgh и т.д.

2.3 Пароли должны содержать символы как минимум из трех следующих групп:

- Строчные латинские буквы: abcd...xyz;
- Прописные латинские буквы: ABCD...XYZ;
- Цифры: 123...90;
- Специальные символы: !%() _+ и т.д.

2.4 Требования к длине пароля:

- Для обычных пользователей - не менее 8 символов;
- Для администраторов (локального\доменного) - не менее 15 символов;
- Для сервисных идентификаторов, разделяемых ключей (shared keys) - не менее 14 символов;
- Для SNMP Community Strings — не менее 10 символов.

2.5 Периодичность смены пароля:

- Административные – каждые 60 дней;
- Пользовательские – каждые 180 дней;
- Сервисные – не реже двух раз в год;

2.6 Пароли не должны храниться и передаваться в незашифрованном виде по публичным сетям (локальная вычислительная сеть, интернет, электронная почта).

2.7 В ходе работы не должны использоваться встроенные идентификаторы. Для них должны быть назначены пароли, отличные от установленных производителем. К ним предъявляются требования, аналогичные требованиям к сервисным паролям.

2.8 Пароли нельзя сообщать и передавать кому-либо, кроме ответственного по информационной безопасности.

2.9 Пароли сервисных идентификаторов должны входить в процедуру управления паролями, включающую хранение их в защищенном месте и периодическую смену (1 раз в год).

3. Требования к настройкам безопасности

3.1 Учетная запись должна блокироваться после 5 неверных попыток доступа не менее чем на 15 минут.

3.2 Запрещается использовать функции «запомнить пароль» в любом программном обеспечении.

4. Требования к паролям сервисных учетных записей

4.1 Пароли для сервисных учетных записей должны формироваться и актуализироваться администратором информационной безопасности, учитываться и храниться в запечатанном конверте в служебном сейфе или запираемом на ключ

шкафу (тумбе). Ключ от сейфа или шкафа хранится у ответственного за информационную безопасность.

4.2 Пароль должен меняться не реже двух раз в год, или немедленно в случае увольнения или смены полномочий администратора информационной безопасности.

4.4 Администратор информационной безопасности, должен ежемесячно проверять наличие конвертов, целостность.

4.5 Вскрытие конвертов может произвести:

- ответственный за информационную систему;
- администратор информационной безопасности.

4.8 Конверты вскрываются одним лицом, с последующей регистрацией в журнале, при этом обязательно информирование администратора или ответственного за информационную безопасность.