Утвержден приказом
ГКУ «Центр занятости населения
города Буинска»

от «24» октября 2019г. № 150

Требования
к идентификаторам и паролям ситуационного центра
ГКУ «Центр занятости населения города Буинска»

Общие положения

Настоящие требования устанавливает порядок и правила генерации, использования, уничтожения идентификатора и пароля в информационных ресурсах ГКУ «Центр занятости населения города Буинска».

Требования к идентификаторам и паролям ГКУ «Центр занятости населения города Буинска»» распространяются на всех сотрудников ГКУ «Центр занятости населения города Буинска» (далее - Пользователь).

Бесконтрольность в определении и использовании пароля может повлечь риск несанкционированного доступа к информации ГКУ «Центр занятости населения города Буинска», что может повлечь модификацию или уничтожение информации и это может нанести вред и ущерб репутации ГКУ «Центр занятости населения города Буинска».

Требования к паролям

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

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.

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.

4. Требования к длине пароля:
для обычных пользователей не менее 6 символов;
для администраторов (локального\доменного) не менее 15 символов.

5. Периодичность смены пароля:
для администраторов (локального\доменного) – каждые 90 дней;
для обычных пользователей – каждые 180 дней.

6. Пароли не должны храниться и передаваться в незашифрованном виде по публичным сетям (интернет, электронная почта).

7. В ходе работы не должны использоваться встроенные идентификаторы. Для них должны быть назначены пароли, отличные от установленных производителем.

8. Пароли нельзя записывать на бумагу, в память телефона и т.д. Нельзя сообщать, передавать кому-либо пароль.

9. Администратору информационной безопасности не реже 1 раза в год проводить проверку соответствия пароля требованиям данной инструкции в присутствии пользователя: пользователь называет свой пароль, а проверяющий осуществляет ввод пароля и его проверку. После такой проверки требуется обязательная и немедленная смена пароля.

Требования к идентификаторам

1. Для каждого идентификатора должна быть определена следующая информация о пользователе: фамилия, имя, отчество пользователя, должность.
2. Учет идентификаторов производится в Журнале учета для идентификаторов (Приложение).

Требования к идентификации

Идентификация должна осуществляться по уникальным учетным записям, которые однозначно идентифицируют пользователя.

Запрещается применять учетные неидентифицируемые учетные записи, например: «user», «пользователь», «administrator» и т.д. без четкого определения принадлежности учетной записи к субъекту доступа.

Требования к настройкам безопасности информационных систем

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

Запрещается использовать функции «Запомнить пароль» в любом программном обеспечении.

Правила и процедуры управления идентификаторами

Администратор информационной безопасности является лицом, ответственным за создание, присвоение и уничтожение идентификаторов пользователей.

Администратор информационной безопасности обязан блокировать или инициировать блокировку идентификаторов пользователей через период времени неиспользования не более 90 дней.

Ответственность

Виновные в нарушении условий настоящего раздела несут ответственность в соответствии с законодательством Российской Федерации.