

Государственное бюджетное профессиональное образовательное учреждение
«Байконурский электрорадиотехнический техникум имени М.И. Неделина»
(ГБ ПОУ «БЭРТТ»)

Принято на заседании
педагогического совета
«12» апреля 2021 г.
протокол № 07

УТВЕРЖДЕНО
приказом ГБ ПОУ «БЭРТТ»
от 20.05.2021 01-03 № 112



**ПОЛОЖЕНИЕ
О ПАРОЛЬНОЙ ЗАЩИТЕ ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ
И ИНОЙ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ
В ГОСУДАРСТВЕННОМ БЮДЖЕТНОМ ПРОФЕССИОНАЛЬНОМ
ОБРАЗОВАТЕЛЬНОМ УЧРЕЖДЕНИИ «БАЙКОНУРСКИЙ
ЭЛЕКТРОРАДИОТЕХНИЧЕСКИЙ ТЕХНИКУМ
ИМЕНИ М.И. НЕДЕЛИНА»**

1. Положение о парольной защите при обработке персональных данных и иной конфиденциальной информации (далее - Положение) регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей в информационных системах (ИС) Государственного бюджетного профессионального образовательного учреждения «Байконурский электрорадиотехнический техникум имени М.И. Неделина» (далее - Учреждение), а также контроль за действиями Пользователей и обслуживающего персонала при работе с паролями.

2. Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями ПС самостоятельно с учетом следующих требований:

длина пароля должна быть не менее 8 символов:

в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, \$, & . * . % и т.п.);

пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.):

при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях;

личный пароль Пользователь не имеет права сообщать никому.

3. 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.

4. В случае, если формирование личных паролей Пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на сотрудников, ответственных за организацию работы АИС в Учреждении. Для генерации «стойких» значений паролей могут применяться специальные программные средства.

5. При наличии технологической необходимости (в случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и т.п.) использования имен и паролей некоторых сотрудников (Пользователей) в их отсутствие, такие сотрудники обязаны сразу же после смены своих паролей сообщать руководителю их новые значения.

6. Полная плановая смена паролей Пользователей должна проводиться регулярно, не реже одного раза в квартал.

7. Внеплановая смена личного пароля или удаление учетной записи Пользователя ИС в случае прекращения его полномочий (увольнение, переход на другую работу и т.п.) должна производиться сотрудниками, отвечающими за работу АИС немедленно после окончания последнего сеанса работы данного Пользователя с системой.

8. Внеплановая полная смена паролей всех Пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и т.п.) администраторов средств защиты и других сотрудников, которым по роду работы были предоставлены полномочия по управлению парольной защитой ИС.

9. Хранение Пользователем своих паролей на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у руководителя в опечатанном конверте.

10. Повседневный контроль за действиями Пользователей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены, хранения и использования, возлагается на сотрудников - администраторов парольной защиты.
