Областное государственное бюджетное образовательное учреждение дополнительного профессионального образования "Томский областной институт повышения квалификации и переподготовки работников образования"

Утверждаю
Ректор ТОИПКРО
_____ О.М. Замятина
«29» апреля 2016г.

Инструкция по организации парольной защиты

Данная инструкция регламентирует организационно-техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационных системах персональных данных (далее – ИСПДн) Областного государственного бюджетного образовательного учреждения дополнительного профессионального образования «Томский областной институт повышения квалификации и переподготовки работников образования» (далее – ТОИПКРО), а также контроль действий пользователей ИСПДн (сотрудников ТОИПКРО) при работе с паролями.

1. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех ИСПДн ТОИПКРО, содержащих механизмы идентификации и аутентификации (подтверждения подлинности) пользователей по значениям паролей, и контроль действий пользователей ИСПДн (сотрудников ТОИПКРО) при работе с паролями возлагается на администраторов соответствующих ИСПДн.

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

- длина пароля должна быть не менее 6 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.

Пользователи ИСПДн (сотрудники ТОИПКРО), владеющие паролями, 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.

3. В случае если формирование личных паролей пользователей ИСПДн осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на Администратора соответствующей ИСПДн. Для генерации «стойких» значений паролей могут применяться специальные программные средства. Система централизованной генерации и распределения паролей должна исключать возможность ознакомления Администраторов ИСПДн, а также Администратора безопасности ИСПДн с паролями пользователей ИСПДн.

4. Полная плановая смена паролей пользователей ИСПДн должна проводиться регулярно, не реже одного раза в год.

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

6. Внеплановая полная смена паролей всех пользователей ИСПДн должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и т.п.) Администратора ИСПДн и других сотрудников, которым по роду работы были предоставлены полномочия по управлению парольной защитой ИСПДн.

7. В случае компрометации личного пароля пользователя ИСПДн должны быть немедленно предприняты меры в соответствии с п.6 или п.7 настоящей Инструкции в зависимости от полномочий владельца скомпрометированного пароля.

8. Хранение пользователями ИСПДн (сотрудниками ТОИПКРО) значений своих паролей на бумажном носителе (персональных ключевых дискет, идентификаторов и т.п.) допускается только в личном сейфе, либо в опечатанном пенале в сейфе Администратора безопасности ИСПДн или руководителя структурного подразделения.

9. Повседневный контроль действий пользователей ИСПДн (сотрудников ТОИПКРО) при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на Администраторов соответствующих ИСПДн, периодический контроль – возлагается на Администратора безопасности ИСПДн.