УТВЕРЖДЕНА
Распоряжением Главы
сельского поселения Красный Яр
муниципального района Красноярский
Самарской области
от 18.08.2022 г № 53

ИНСТРУКЦИЯ ПО ОРГАНИЗАЦИИ ПАРОЛЬНОЙ ЗАЩИТЫ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

Настоящая Инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационных системах персональных данных (далее – ИСПДн) Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области (далее – администрации), а также контроль за действиями пользователей и обслуживающего персонала ИСПДн при работе с паролями.

1. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПДн администрации и контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями возлагается на ответственного за организацию обработки ПДн, являющегося специалистом по защите информации.

2. Личные пароли выбираются пользователями автоматизированной системы самостоятельно либо могут генерироваться и распределяться централизованно с учетом следующих требований:

- длина пароля должна быть не менее 6 символов;
- в числе символов пароля обязательно должны присутствовать буквы латинского алфавита в верхнем и нижнем регистрах и цифры, а также могут использоваться специальные символы (@, #, $, &, *, % и т.п.);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии пользователей, наименования АРМ, учетные записи и т.д.), а также общепринятые сокращения (USER, PASSWORD, MANAGER и т.п. и производные от них);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 3 позициях.

3. Владельцы паролей должны быть ознакомлены под роспись с настоящей инструкцией по форме согласно приложению и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

4. При наличии (в случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и т.п.) технологической необходимости использования имен и паролей некоторых сотрудников в их отсутствие, такие сотрудники обязаны сразу же после смены своих паролей их новые значения (вместе с именами соответствующих учетных записей) в запечатанном конверте передавать на хранение ответственному за организацию обработки ПДн. Опечатанные конверты (пеналы) с паролями исполнителей должны храниться в сейфе.

5. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в месяц.

6. Внеплановая смена личного пароля или удаление учетной записи пользователя информационной системы в случае прекращения его полномочий (увольнение, переход на другую работу) должна производиться ответственным за организацию обработки ПДн, ответственным за организацию парольной защиты, немедленно после окончания последнего сеанса работы данного пользователя с системой.

7. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение и другие обстоятельства) ответственного за организацию обработки ПДн, ответственного за организацию парольной защиты, и других сотрудников, которым по роду служебной деятельности были предоставлены полномочия по управлению парольной защитой ИС.

8. В случае компрометации личного пароля пользователя информационной системы должны быть немедленно предприняты меры в соответствии с пунктом 4 или пунктом 5 настоящей Инструкции в зависимости от полномочий владельца скомпрометированного пароля.

9. Хранение сотрудником значений своих паролей на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у Ответственного за организацию обработки ПДн, ответственного за организацию парольной защиты, или начальника отдела в опечатанном виде.

10. Каждый пользователь несет ответственность за неразглашение личного пароля третьим лицам и сохранность персонального идентификатора.

11. Повседневный контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на начальников отделов, периодический контроль возлагается на ответственного за организацию обработки ПДн, ответственного за организацию парольной защиты.