Приложение № 2
к приказу «Об обеспечении безопасности персональных данных в информационных системах персональных данных ФГБУЗ ММЦ им. Н.И. Пирогова ФМБА России» № 01-147 от 12.07.2022

Инструкция по организации парольной защиты персональных данных и конфиденциальной информации в информационных системах Федерального государственного бюджетного учреждения здравоохранения «Мурманский многопрофильный центр имени Н.И. Пирогова Федерального медико-биологического агентства»

1. Общие положения

Данная инструкция регламентирует:

- организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационных системах персональных данных Федерального государственного бюджетного учреждения здравоохранения «Мурманский многопрофильный центр имени Н.И. Пирогова Федерального медико-биологического агентства» (далее Учреждение): ПО «Парус Бюджет 8», «1С-Предприятие 8», МИС «Медиалог», МИС «ЭконБол 3», ФГИС «ЕВМИАС» (далее - ИСПДн);
- контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.

2. Технологический процесс организации парольной защиты

2.1. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПДн и контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями возлагается на администратора ИСПДн.

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

- длина пароля не менее шести символов;
- алфавит пароля не менее 70 символов;
- максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки от 3 до 4 попыток;
- блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации от 15 до 60 минут;

– смена паролей не более чем через 120 дней;

– 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, дни рождения, наименования ИСПДн и т.д.), а также общепринятые сокращения (USER, QWERTY и т.п.);

– при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях.

2.3. Личный пароль пользователь не имеет права сообщать никому.

2.4. 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.

2.5. Если формирование личных паролей пользователей осуществляется централизованно – ответственность за правильность их формирования и распределения возлагается на администратора ИСПДн. Для генерации «стойких» значений паролей могут применяться специальные программные средства. Система централизованной генерации и распределения паролей должна исключать возможность ознакомления самого администратора ИСПДн с паролями других сотрудников.

2.6. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в 120 дней.

2.7. Внеплановая смена личного пароля или удаление учетной записи пользователя ИСПДн в случае прекращения его полномочий (увольнение, переход на другую работу, в т.ч. в иной департамент), должна производиться администратором ИСПДн немедленно после окончания последнего сеанса работы данного пользователя с системой.

2.8. Внеплановая, полная смена паролей всех пользователей должна производиться в случае прекращения полномочий сотрудника (сотрудников), которым по роду работы были предоставлены полномочия по управлению парольной защитой подсистем ИСПДн.

2.9. В случае компрометации личного пароля пользователя ИСПДн должны быть немедленно предприняты меры в соответствии с п.2.7 или п.2.8 настоящей Инструкции в зависимости от полномочий владельца скомпрометированного пароля.

2.10. Хранение сотрудником своего пароля на бумажном носителе в местах, доступных для третьих лиц, не допускается.

2.11. Периодический контроль за действиями пользователей и обслуживающего персонала ИСПДн при работе с паролями, соблюдение порядка их смены, хранения и использования, возлагается на администратора безопасности.