

**Государственное казенное учреждение здравоохранения
Детский санаторий «ТОПОЛЁК»
Министерства Здравоохранения Краснодарского края**

УТВЕРЖДАЮ

Главный врач

ГКУЗ «Детский санаторий «Тополек»

/ М. А. Мугу /

12 2021 г.



**ИНСТРУКЦИЯ
ПО ОРГАНИЗАЦИИ ПАРОЛЬНОЙ ЗАЩИТЫ
ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ**

Данная инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационных системах персональных данных (далее – ИСПДн) ГКУЗ «Детский санаторий «Тополек», а также контроль действий пользователей и обслуживающего персонала системы при работе с паролями.

1. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПДн ГКУЗ «Детский санаторий «Тополек» и контроль действий исполнителей и обслуживающего персонала ИСПДн при работе с паролями возлагается на сотрудников комитета информатизации и связи - администраторов средств защиты, содержащих механизмы идентификации и аутентификации (подтверждения подлинности) пользователей по значениям паролей.

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.

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.

3. В случае если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на уполномоченных сотрудников. Для генерации «стойких» значений паролей могут применяться специальные программные средства. Система централизованной генерации и распределения паролей должна исключать возможность ознакомления самих уполномоченных сотрудников, а также ответственных за информационную безопасность в подразделениях с паролями других сотрудников ГКУЗ «Детский санаторий «Тополек».

4. Полная плановая смена паролей пользователей 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 внутри ГКУЗ «Детский санаторий «Тополек» и т.п.) должна производиться администраторами соответствующих средств защиты немедленно после окончания последнего сеанса работы данного пользователя с системой.

6. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри ГКУЗ «Детский санаторий «Тополек» и другие обстоятельства) администраторов средств защиты и других сотрудников, которым по роду работы были предоставлены полномочия по управлению парольной защитой подсистем ИСПДн.

7. В случае компрометации личного пароля пользователя ИСПДн должны быть немедленно предприняты меры в соответствии с п.5 или п.6 настоящей Инструкции в зависимости от полномочий владельца скомпрометированного пароля.

8. Хранение сотрудником ГКУЗ «Детский санаторий «Тополек» значений своих паролей на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у ответственного за информационную безопасность или руководителя подразделения в опечатанном личной печатью пенале (возможно вместе с персональными ключевыми дискетами и идентификатором).

9. Повседневный контроль действий исполнителей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на ответственных за информационную безопасность в подразделениях (руководителей подразделений), периодический контроль – возлагается на Администратора безопасности ИСПДн и ответственного за обеспечение безопасности ИСПДн.