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

УТВЕРЖДАЮ
Главный врач
ГКУЗ «Детский санаторий «Тополек»
_____ / М. А. Мугу /
«27» 12 2021 г.

ИНСТРУКЦИЯ ПОЛЬЗОВАТЕЛЯ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

1 Общие положения

1.1. Пользователь ИСПДн (далее – Пользователь) осуществляет обработку персональных данных в информационной системе персональных данных.

1.2. Пользователем является сотрудник ГКУЗ «Детский санаторий «Тополек», участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.

1.3. Пользователь несет персональную ответственность за свои действия.

1.4. Пользователь в своей работе руководствуется настоящей инструкцией, локальными актами ГКУЗ «Детский санаторий «Тополек», руководящими и нормативными документами в сфере защиты конфиденциальной информации и персональных данных в частности.

1.5. Методическое руководство работой пользователя осуществляется ответственным за обеспечение защиты персональных данных.

2 Должностные обязанности

Пользователь обязан:

2.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации.

2.2. Выполнять на автоматизированном рабочем месте (АРМ) только те процедуры, которые определены для него в соответствии с правила разграничения доступа.

2.3. Знать и соблюдать установленные требования по режиму обработки персональных данных, учету, хранению и пересылке носителей информации, обеспечению безопасности ПДн, а также руководящих и организационно-распорядительных документов.

2.4. Соблюдать требования парольной политики (Инструкция по организации парольной защиты).

2.5. Соблюдать правила при работе в сетях общего доступа и (или) международного обмена – Интернет и других (Инструкция по работе в сети международного информационного обмена).

2.6. Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами, шторы на оконных проемах должны быть завешаны (жалюзи закрыты).

2.7. Обо всех выявленных нарушениях, связанных с информационной безопасностью ГКУЗ «Детский санаторий «Тополек», а также для получений консультаций по вопросам информационной безопасности, необходимо обратиться к ответственному лицу – Администратору безопасности.

2.8. Для получения консультаций по вопросам работы и настройке элементов ИСПДн необходимо обращаться к Администратору ИСПДн по внутреннему телефону 1111.

2.9. Пользователям запрещается:

- Разглашать защищаемую информацию третьим лицам.

- Копировать защищаемую информацию на внешние носители без разрешения своего руководителя.

- Самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств.

- Несанкционированно открывать общий доступ к папкам на своей рабочей станции.

- Запрещено подключать к рабочей станции и корпоративной информационной сети личные внешние носители и мобильные устройства.

- Отключать (блокировать) средства защиты информации.

- Обрабатывать на АРМ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к ИСПДн.

- Сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИСПДн.

- Привлекать посторонних лиц для производства ремонта или настройки АРМ, без согласования с ответственным за обеспечение защиты персональных данных.

2.10. При отсутствии визуального контроля за рабочей станцией: доступ к компьютеру должен быть немедленно заблокирован.

2.11. Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий, в рамках возложенных, в пределах возложенных на него функций.

2.12. Не разглашать информацию, к которой они допущены, в том числе сведения о средствах защиты, ключевых документах к ним и других мерах защиты;

2.13. Соблюдать требования к обеспечению безопасности персональных данных, требования к обеспечению безопасности криптосредств и ключевых документов к ним;

2.14. Сообщать о ставших им известными попытках посторонних лиц получить сведения об используемых средствах защиты или ключевых документах к ним;

2.15. Немедленно уведомлять оператора о фактах утраты или недостачи криптосредств, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых персональных данных.