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 АДМИНИСТРАТОРА ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

1 Общие положения

1.1. Администратор ИСПДн (далее – Администратор) назначается приказом Главного врача ГКУЗ «Детский санаторий «Тополек», на основании Регламента разграничения прав доступа к обрабатываемым персональным данным.

1.2. Администратор подчиняется Главному врачу ГКУЗ «Детский санаторий «Тополек».

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

1.4. Администратор отвечает за обеспечение устойчивой работоспособности элементов ИСПДн и средств защиты, при обработке персональных данных.

1.5. Методическое руководство работой ГКУЗ «Детский санаторий «Тополек» осуществляется ответственным за обеспечение безопасности персональных данных.

2 Должностные обязанности

Администратор 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. Обеспечивать установку, настройку и своевременное обновление элементов ИСПДн:

- программного обеспечения АРМ и серверов (операционные системы, прикладное и специальное ПО);
- аппаратных средств;

2.3. Обеспечивать работоспособность элементов ИСПДн и локальной вычислительной сети.

2.4. Осуществлять контроль за порядком учета, создания, хранения и использования резервных и архивных копий массивов данных, машинных (выходных) документов.

2.5. Обеспечивать функционирование и поддерживать работоспособность средств защиты в рамках возложенных на него функций.

2.6. В случае отказа работоспособности технических средств и программного обеспечения элементов ИСПДн, в том числе средств защиты информации, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

2.7. Проводить периодический контроль принятых мер по защиты, в пределах возложенных на него функций.

2.8. Хранить, осуществлять прием и выдачу персональных паролей пользователей, осуществлять контроль за правильностью использования персонального пароля пользователями ИСПДн.

2.9. Обеспечивать постоянный контроль за выполнением пользователями установленного комплекса мероприятий по обеспечению безопасности информации.

2.10. Информировать ответственного за обеспечение защиты персональных данных о фактах нарушения установленного порядка работ и попытках несанкционированного доступа к информационным ресурсам ИСПДн.

2.11. Требовать прекращения обработки информации, как в целом, так и для отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования ИСПДн или средств защиты.

2.12. Обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации обслуживания технических средств и отправке их в ремонт. Техническое обслуживание и ремонт средств вычислительной техники, предназначенных для обработки персональных данных, проводятся организациями, имеющими соответствующие лицензии. При проведении технического обслуживания и ремонта запрещается передавать ремонтным организациям узлы и блоки с элементами накопления и хранения информации.

2.13. Присутствовать при выполнении технического обслуживания элементов ИСПДн сотрудниками сторонних организаций.

2.14. Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий.

2.15. Присутствовать при установке и настройке сотрудниками сторонних организаций, имеющих соответствующие лицензии, средств защиты информации на объекты информатизации ИСПДн. А также по завершению данных работ провести проверку на соответствие заданным требованиям, осуществить приемку выполненных работ.

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

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

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

2.19 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.