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

УТВЕРЖДАЮ
Главный врач
ГКУЗ «Детский санаторий «Тополек»
_____ / М. А. Мугу /
«21» 12 2021 г.

ИНСТРУКЦИЯ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

1 Общие положения

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

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

1.3. Администратор безопасности 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.

1.4. Администратор безопасности отвечает за поддержание необходимого уровня безопасности объектов защиты.

1.5. Администратор безопасности является ответственным должностным лицом ГКУЗ «Детский санаторий «Тополек», уполномоченным на проведение работ по поддержанию достигнутого уровня защиты информационной системы персональных данных (далее – ИСПДн) и ее ресурсов на этапах промышленной эксплуатации и модернизации.

1.6. Администратор безопасности должен иметь специальное рабочее место, размещенное в здании, где расположена ГКУЗ «Детский санаторий «Тополек» так, чтобы исключить несанкционированный доступ к нему посторонних лиц и других пользователей.

1.7. Рабочее место Администратора безопасности должно быть оборудовано средствами физической защиты (личный сейф, железный шкаф или другое), подключением к ИСПДн, а также средствами контроля за техническими средствами защиты.

1.8. Администратор безопасности осуществляет методическое руководство пользователей и Администраторов ИСПДн, в вопросах обеспечения безопасности персональных данных.

1.9. Требования администратора информационной безопасности, связанные с выполнением им своих должностных обязанностей, обязательны для исполнения всеми пользователями обрабатывающих персональные данные.

1.10. Администратор безопасности несет персональную ответственность за качество проводимых им работ по контролю действий пользователей при работе в ИСПДн, состояние и поддержание установленного уровня защиты ИСПДн.

2 Должностные обязанности

Администратор безопасности 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. Осуществлять сопровождение технических средств защиты.

2.3. Участвовать в контрольных и тестовых испытаниях и проверках элементов ИСПДн.

2.4. Участвовать в приемке новых программных средств.

2.5. Обеспечить доступ к защищаемой информации пользователям ИСПДн согласно их правам доступа при получении оформленного соответствующим образом разрешения.

2.6. Уточнять в установленном порядке обязанности пользователей ИСПДн по обработке объектов защиты.

2.7. Вести контроль над процессом осуществления резервного копирования объектов защиты.

2.8. Осуществлять контроль над выполнением Плана мероприятий по защите персональных данных.

2.9. Анализировать состояние защиты ИСПДн и ее отдельных подсистем.

2.10. Контролировать неизменность состояния средств защиты их параметров и режимов защиты.

2.11. Контролировать физическую сохранность средств и оборудования ИСПДн.

2.12. Контролировать исполнение пользователями ИСПДн введенного режима безопасности, а так же правильность работы с элементами ИСПДн и средствами защиты.

2.13. Контролировать исполнение пользователями парольной политики.

2.14. Контролировать работу пользователей в сетях общего пользования и (или) международного обмена.

2.15. Своевременно анализировать журнал учета событий, регистрируемых средствами защиты, с целью выявления возможных нарушений.

2.16. Не допускать установку, использование, хранение и размножение в ИСПДн программных средств, не связанных с выполнением функциональных задач.

2.17. Не допускать к работе на элементах ИСПДн посторонних лиц.

2.18. Осуществлять периодические контрольные проверки рабочих станций и тестирование правильности функционирования средств защиты ИСПДн.

2.19. Оказывать помощь пользователям ИСПДн в части применения средств защиты и консультировать по вопросам введенного режима защиты.

2.20. Периодически представлять руководству отчет о состоянии защиты ИСПДн и о нештатных ситуациях на объектах ИСПДн и допущенных пользователями нарушениях установленных требований по защите информации.

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

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

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

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

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

2.26 Немедленно уведомлять Главного врача 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.