Государственное бюджетное профессиональное образовательное учреждение Республики Карелия «Олонецкий техникум»

УТВЕРЖДАЮ:
Директор _____ С. В. Седлецкий
«29» декабря 20 16 год

Инструкция
ответственного за работу с персональными данными
и ответственного за техническую защиту информации,
содержащей персональные данные

1. Общие положения.

1.1. Ответственные за работу и техническую защиту персональных данных (далее – Администраторы безопасности) назначаются приказом руководителя государственного бюджетного профессионального образовательного учреждения Республики Карелия «Олонецкий техникум» (далее – Организация).

1.2. Администраторы безопасности подчиняются руководителю Организации.

1.3. Администраторы безопасности в своей работе руководствуются настоящей инструкцией, Концепцией информационной безопасности и Политикой информационной безопасности Организации, руководящими и нормативными документами ФСТЭК России, внутренними инструкциями и распоряжениями, регламентирующими порядок действий по защите информации.

1.4. Администраторы безопасности отвечают за поддержание необходимого уровня безопасности данных, указанных в перечне подлежащих защите сведений.

1.5. Администраторы безопасности являются ответственными должностными лицами Организации, уполномоченными на проведение работ по технической защите информации и поддержанию достигнутого уровня защиты информационных систем персональных данных (далее – ИСПДн) и ее ресурсов на этапах промышленной эксплуатации и модернизации.

1.7. Рабочее место ответственного за работу с ПДн должно быть оборудовано средствами физической защиты (личный сейф, железный шкаф или другое), подключением к ИСПДн.

1.8. Администраторы безопасности осуществляют методическое руководство пользователей ИСПДн в вопросах обеспечения безопасности персональных данных.

1.9. Требования Администраторов безопасности, связанные с выполнением им своих должностных обязанностей, обязательны для исполнения всеми пользователями ИСПДн.

1.10. Администраторы безопасности несут 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

Администраторы безопасности обязаны:

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. Участвовать в установке, настройке и сопровождении 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. Обеспечивать доступ к защищаемой информации пользователям ИСПДн согласно их правам доступа.

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.

Ответственный за защиту информации Т. Г. Прохорова
“____” _____ 20__г.

Ответственный за техническую защиту информации А. Г. Андреев
“____” _____ 20__г.