УТВЕРЖДЕНО
приказом от «__» _____ 2018г. № 99-ОД

Инструкция
ответственного за информационную безопасность
информационной системы персональных данных

1. Общие положения

1.1. Настоящая инструкция определяет функции ответственного за информационную безопасность информационной системы персональных данных в ГБОУ РК ЦДК (далее – ОУ) по вопросам обеспечения конфиденциальности при проведении в ИСПДн работ с использованием персональных данных.
1.2. Ответственный за информационную безопасность назначается приказом директора.

2. Основные функции ответственного за информационную безопасность

2.1. Контроль за выполнением установленного комплекса мероприятий по обеспечению безопасности персональных данных в ИСПДн.
2.2. Организация доступа пользователей ИСПДн к защищаемым информационным ресурсам ИСПДн.
2.3. Обеспечение целостности данных в защищаемом сегменте компьютерной сети.
2.4. Обеспечение резервного копирования данных защищаемого сегмента компьютерной сети.
2.5. Установка, настройка и сопровождение средств защиты информации.
2.6. Выполнение регламентных работ по обслуживанию средств защиты информации в соответствии с их руководствами по эксплуатации.
2.7. Анализ событий информационной безопасности, получаемых от средств защиты информации, а также обеспечение необходимых мер по устранению ситуаций нарушения информационной безопасности в будущем (оперативное реагирование на поступающие сигналы о нарушениях установленных правил доступа, анализ журналов регистрации событий безопасности и т.п.).
2.8. Организация мероприятий по предотвращению несанкционированных модификаций программного обеспечения, добавления новых функций, несанкционированного доступа к информации, аппаратуре и другим общим ресурсам защищаемой ИСПДн.
2.9. Периодическое тестирование функций установленных средств защиты информации при изменении программной среды и/или полномочий пользователей.
2.10. Восстановление настроек средств защиты информации после сбоев.
2.11. Контроль за появлением новых версий программного обеспечения средств защиты.
2.12. Введение журналов, необходимых для учета процессов при функционировании защищаемого сегмента компьютерной сети.
2.13. Выполнение требований по парольной защите ИСПДн в соответствии с настоящей Инструкцией.
2.14. Проведение инструктажа пользователей ИСПДн по внедряемым программным и (или) техническим средствам защиты.
2.15. Контроль актуальности сертификатов ФСТЭК и ФСБ для средств защиты информации.
2.16. Участие в разработке исходных данных и постановке задач на модернизацию защищаемого сегмента компьютерной сети.
2.17. Документирование изменений в конфигурации ИСПДн.

3. Порядок парольной защиты в ИСПДн

3.1. Ответственный за информационную безопасность осуществляет организационно-техническое обеспечение процессов установки и смены действия паролей пользователей ИСПДн.

3.2. Личные пароли пользователей ИСПДн должны генерироваться и распределяться в соответствии с п.3 раздела 5 документа
3.3. Внеплановая смена пароля пользователя ИСПДн должна производиться в случае прекращения полномочий работника ОУ (увольнение, переход на другую должность/организацию и другие обстоятельства) в соответствии с п.3 раздела 5 документа.
3.4. В случае компрометации пароля пользователя ИСПДн ответственный за информационную безопасность выясняет обстоятельства потери и информирует о произошедшем начальство в соответствии с п.1 раздела 5 документа.
3.5. Хранение значений паролей осуществляется в соответствии с требованиями п.3 раздела 5 документа

4. Порядок программно-технического обслуживания ИСПДн

4.1. Ответственный за информационную безопасность осуществляет контроль за целостностью печатей (пломб) на технических средствах ИСПДн (при наличии таковых), а также за соответствием установленного в ИСПДн программного обеспечения и технических средств, заявленных в техническом паспорте на ИСПДн.
4.2. Все работы по внесению изменений в аппаратно-программную конфигурацию ИСПДн проводятся системными администраторами и администраторами ИСПДн, определенными документом «Матрица доступа к защищаемым информационным ресурсам ИСПДн», по согласованию с ответственным за информационную безопасность .
Произведенные изменения заносятся в технический паспорт на ИСПДн.
4.3. Отправка технических средств, входящих в состав ИСПДн, их ремонт или замена на новые производятся по согласованию с органом, выдавшим «Аттестат соответствия требованиям по безопасности информации» на ИСПДн.

5. Перечень нормативных документов, использованных при разработке данной инструкции.

5.1 Регламент по проведению контрольных мероприятий и реагированию на инциденты информационной безопасности (Инструкция пользователя ИСПДн на случай возникновения внештатных ситуаций).
5.2 Разрешительная система доступа к ПДн.
5.3 Инструкция по организации парольной защиты.
5.4 Порядок резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации (СЗИ).

ОЗНАКОМЛЕН
Ответственный
за информационную безопасность _____ _____
(подпись) (расшифровка)