

Утверждаю

Директор

МБУ ДО ЦРТДЮ

Максютов В.Т.

Приказ №

од от

2024г.

ИНСТРУКЦИЯ

ответственного по безопасности информации МБУ ДО ЦРТДЮ

1. Общие положения

Настоящая инструкция определяет права и обязанности ответственного по безопасности информации.

Ответственный по безопасности информации назначается приказом директора и отвечает за обеспечение устойчивой работы и информационной безопасности МБУ ДО ЦРТДЮ.

Ответственный по безопасности информации обеспечивает правильность использования информационных ресурсов и нормальное функционирование защитных механизмов автоматизированных систем (далее - АС). Настоящая Инструкция является дополнением и не исключает обязательного выполнения требований других действующих нормативных документов по вопросам обеспечения защиты информации ограниченного доступа.

2. Функции администратора безопасности информации

Администратор безопасности:

осуществляет контроль, за целевым использованием АС и входящих в состав АС всех внешних устройств;

осуществляет контроль доступа пользователей к информационным и техническим ресурсам АС, производит персонализацию пользователей путем присвоения им персональных идентификаторов и паролей доступа временного действия;

устанавливает права доступа пользователей к информационным и техническим ресурсам АС;

осуществляет регулярную замену паролей доступа пользователей к ресурсам АС и их доведение до соответствующих категорий пользователей;

осуществляет настройку и сопровождение подсистем регистрации и учета действий пользователей АС, производит настройку операционной системы для выполнения регистрационно-учетных функций;

своевременно информирует руководителя образовательной организации о выявленных несанкционированных действиях пользователей АС;

обеспечивает целостность и сохранность защищаемой информации: проводит периодическое тестирование защитных механизмов АС;

следит за изменением программной среды АС и полномочиями пользователей;

проводит резервное копирование файлов с настройками операционной системы;

производит восстановление программной среды АС с имеющихся лицензионных дистрибутивов программного обеспечения, либо с резервных копий в части, касающейся настройки защитных механизмов операционной системы и привилегий пользователей по доступу к ресурсам АС;

проводит своевременное обновление антивирусного программного обеспечения на АС;

в случае обнаружения вирусов принимает меры по выявлению и уничтожению вредоносных программ и недопущению их дальнейшего распространения;

осуществляет очистку областей памяти на магнитных носителях информации в соответствии с установленной технологией.

3. Администратор безопасности информации имеет право:

контролировать работу пользователей на АС;

требовать прекращения обработки информации, как в целом, так и отдельными пользователями, в случае выявления нарушений установленного порядка работ или нарушения функционирования АС.

4. Администратор безопасности информации обязан:

обеспечивать функционирование и поддерживать работоспособность АС в пределах возложенных на него функций;

проводить инструктаж пользователей по порядку и правилам работы на АС, а также по правилам использования информационных ресурсов;

проводить регулярное резервное копирование информации в пределах установленных функций;

своевременно информировать руководителя образовательной организации о фактах нарушения установленного порядка работ и попытках несанкционированного доступа к информационным ресурсам АС;

назначать и своевременно изменять пароли пользователей;

проводить тестирование защитных механизмов операционной системы на АС.