

ПОЛОЖЕНИЕ

Об информационной безопасности несовершеннолетних в ГКУ СО КК «Динской социально-реабилитационный центр для несовершеннолетних»

1. Общие положения

1.1. Настоящее положение об информационной безопасности (далее-Положение) ГКУ СО КК «Динской социально-реабилитационный центр для несовершеннолетних» разработано в соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральным законом от 29.12.2011 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию».

1.2. Настоящее Положение определяет задачи, функции, обязанности, ответственность и права ответственных за информационную безопасность.

1.3. Ответственные за информационную безопасность назначаются приказом директора учреждения.

1.4. Ответственные за информационную безопасность подчиняются директору учреждения.

1.5. Ответственные за информационную безопасность в своей работе руководствуются настоящим Положением.

1.6. Ответственные за информационную безопасность в пределах своих функциональных обязанностей обеспечивают безопасность информации, обрабатываемой, передаваемой и хранимой при помощи информационных средств ГКУ СО КК «Динской СРЦН».

2. Основные задачи и функции ответственных за информационную безопасность

2.2. Основными задачами ответственных за информационную безопасность являются:

2.1.1. Организация эксплуатации технологических и программных средств защиты информации.

2.1.2. Технический контроль работы средств и систем защиты информации.

2.1.3. Организация и контроль резервного копирования информации на сервере.

2.2. Ответственные за информационную безопасность выполняют следующие основные функции:

2.2.1. Разработка инструкций по информационной безопасности, инструкции по организации антивирусной защиты, инструкции по безопасной работе в Интернете.

2.2.2. Обеспечение несовершеннолетних персональным компьютером (далее- ПК) правилам безопасной обработки информации и правилам работы со средствами защиты информации.

2.2.3. Организация антивирусного контроля магнитных носителей информации и файлов электронной почты, поступающей в ГКУ СО КК «Динской СРЦН».

2.2.4. Текущий контроль работоспособности и эффективности функционирования эксплуатируемых программных и технологических средств защиты информации.

2.2.5. Контроль целостности эксплуатируемого на ПК программного обеспечения с целью выявления несанкционированных изменений в нем.

2.2.6. Контроль за санкционированным изменением программного обеспечения, заменой и ремонт ПК.

2.2.7. Контроль пользования Интернетом.

3. Обязанности ответственных за информационную безопасность

3.1. Обеспечивать функционирование и поддерживать работоспособность средств и систем защиты информации в пределах возложенных на них обязанностей. Немедленно докладывать директору учреждения о выявленных нарушениях и несанкционированных действиях пользователей, а также принимать необходимые меры по устранению нарушений.

3.2. Проводить инструктаж сотрудников и пользователей ПК по правилам работы с используемыми средствами и системы защиты информации.

3.3. Создавать и удалять учетные записи пользователей.

3.4. Отслеживать работу антивирусных программ, проводить один раз в неделю полную проверку компьютеров на наличие вирусов.

3.5. Вести учет пользователей «точки доступа к Интернету». В случае необходимости лимитировать время работы пользователей в Интернете и объем скачиваемой информации. необ- скачи-

4. Права ответственных лиц за информационную безопасность

4.1. Требовать от сотрудников и пользователей компьютерной техники безусловного соблюдения установленной технологии и выполнения инструкций по обеспечению безопасности и защиты информации, содержащей сведения ограниченного распространения.

4.2. Готовить предложения по совершенствованию используемых систем защиты информации и ответственных компонентов.

5. Ответственность лиц информационную безопасность

5.1. На ответственных лиц за информационную безопасность возлагается персональная ответственность за качество проводимых ими работ по обеспечению защиты информации в соответствии с функциональными обязанностями, определенными настоящим Положением.