

Принято
Педагогическим советом
Протокол № 3
от «12» января 2016 г.

УТВЕРЖДАЮ Директор
МАУ ДО «ДЮЦ «Спутник»
Овчинникова О.Н. Томчик
Приказ № 19-с/д
От «12» января 2016 г.



**ПОЛОЖЕНИЕ
ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
МУНИЦИПАЛЬНОГО АВТОНОМНОГО УЧРЕЖДЕНИЯ
ДОПОЛНИТЕЛЬНОГО ОБРАЗОВАНИЯ
«ДЕТСКО-ЮНОШЕСКИЙ ЦЕНТР «СПУТНИК»**

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение об информационной безопасности (далее по тексту Положение) муниципального автономного учреждения дополнительного образования «Детско-юношеский центр «Спутник» (далее - Центр), 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».

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

1.3. Ответственные за информационную безопасность назначаются приказом директора Центра.

1.4. Ответственные за информационную безопасность подчиняются директору Центра. 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 в Центре.

**2. ОСНОВНЫЕ ЗАДАЧИ И ФУНКЦИИ, ОТВЕТСТВЕННЫХ ЗА
ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ**

2.1. Основными задачами ответственных за информационную безопасность являются: 2.1.1. Организация эксплуатации технических и программных средств защиты информации.

2.1.2. Текущий контроль работы средств и систем защиты информации.

2.1.3. Организация и контроль резервного копирования информации на сервере ЛВС.

2.1.4. Ответственные за информационную безопасность выполняют следующие основные функции:

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

2.1.6. Обучение персонала и пользователей ПК правилам безопасной обработки информации и правилам работы со средствами защиты информации.

2.1.7. Организация антивирусного контроля магнитных носителей информации и файлов электронной почты, поступающих в Центр.

2.1.8. Текущий контроль работоспособности и эффективности

2.1.8. функционирования эксплуатируемых программных и технических средств защиты информации.

2.1.9. Контроль целостности эксплуатируемого на ПК программного обеспечения с целью выявления несанкционированных изменений в нём.

2.1.10. Контроль за санкционированным изменением программного обеспечения, заменой и ремонтом ПК.

2.1.11 Контроль пользования Интернетом.

2.1.12

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 Центра о выявленных нарушениях и несанкционированных действиях пользователей и сотрудников, а также принимать необходимые меры по устранению нарушений.

2.2. Совместно с программистом принимать меры по восстановлению работоспособности средств и систем защиты информации.

2.3. Проводить инструктаж сотрудников и пользователей ПК по правилам работы с используемыми средствами и системами защиты информации.

2.4. Создавать и удалять учетные записи пользователей.

2.5. Администрировать работу сервера ЛВС, размещать и классифицировать информацию на сервере ЛВС.

2.6. Устанавливать по согласованию с директором Центра критерии доступа пользователей на сервер ЛВС.

2.7. Формировать и представлять пароли для новых пользователей, администрировать права пользователей.

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

3.9.Выполнять регулярно резервное копирование данных на сервере, при необходимости восстанавливать потерянные или поврежденные данные.

3.Ю.Вести учет пользователей «точки доступа к Интернету». В случае необходимости лимитировать время работы пользователя в Интернете и объем скачиваемой информации.

3.11.Сообщать незамедлительно директора Центра о выявлении случаев несанкционированного доступа в Интернет.

4.ПРАВА ОТВЕТСТВЕННЫХ 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 и электронных платежей.

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

5.ОТВЕТСТВЕННОСТЬ ОТВЕТСТВЕННЫХ ЛИЦ ЗА ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ

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