

Федеральное государственное автономное образовательное учреждение  
высшего образования  
Национальный исследовательский технологический университет «МИСИС»

УТВЕРЖДАЮ

Проректор по образованию

А.И. Воронин

«17» марта 2025 г.

Дополнительная общеобразовательная общеразвивающая  
программа

**«Основы информационной безопасности»**

НАПРАВЛЕННОСТЬ: ТЕХНИЧЕСКАЯ

Уровень: ознакомительный

Возраст обучающихся 14 – 16 лет

Срок реализации: 12 академических часов



Разработчик:  
И.В. Резниченко,  
инспектор по информационным  
системам УПНиП НИТУ МИСИС

Москва 2025

# 1. Пояснительная записка

## 1.1 Характеристика образовательной программы

Данная образовательная программа разработана для формирования у обучающихся школьников 7-8 классов базовых знаний, умений и навыков в области информационной безопасности (ИБ). Программа направлена на повышение осведомленности о существующих угрозах в информационном пространстве, формирование ответственного отношения к личной информации и развитие практических навыков защиты от наиболее распространенных киберугроз.

**Направленность программы:** техническая.

**Уровень освоения:** ознакомительный.

**Новизна программы** Новизна данной программы заключается в ее акценте на современных и актуальных угрозах, с которыми сталкиваются подростки в сети Интернет, использовании интерактивных методов обучения на основе реальных кейсов и симуляций, персонализированном подходе и учете индивидуальных потребностей учащихся, а также применении современных образовательных технологий и ориентации на формирование практических навыков, необходимых в повседневной жизни.

**Педагогическая целесообразность** «Основы информационной безопасности» обусловлена ее актуальностью, соответствием возрастным особенностям учащихся, направленностью на формирование ключевых компетенций, воспитательным потенциалом и практической значимостью. Программа позволяет учащимся получить необходимые знания, умения и навыки для безопасного и эффективного использования информационных технологий, защиты себя и своих близких от онлайн-угроз, а также стать более ответственными и компетентными гражданами информационного общества.

## 1.2. Цель и задачи программы

**Цель** - Формирование у обучающихся базовых знаний и навыков в области информационной безопасности и защиты персональных данных.

**Задачами** программы являются формирования у обучающихся навыков и умений в области защиты информации.

*Образовательные задачи:*

### 1. Ознакомление с основополагающими понятиями:

- Сформировать понимание ключевых терминов: информация, информационная система, информационная безопасность, угроза, уязвимость, риск, конфиденциальность, целостность, доступность.
- Ознакомить с классификациями информации по различным критериям (по степени конфиденциальности, по форме представления и т.д.).

### 2. Изучение типов угроз и атак:

- Классифицировать угрозы информации (вредоносное ПО, фишинг, социальная инженерия, атаки типа "отказ в обслуживании", утечки данных).
- Изучить механизмы реализации различных видов атак (как работает фишинговая схема, как распространяются вирусы).
- Выявить наиболее распространенные и актуальные угрозы для целевой аудитории (например, кибербуллинг, кража аккаунтов в онлайн-играх).

### 3. Ознакомление со средствами и методами защиты:

- Изучить классификацию средств защиты информации (технические, программные, организационные, физические).

- Рассмотреть принципы работы основных средств защиты: антивирусное ПО, брандмауэры, системы аутентификации, шифрование, резервное копирование.
- Ознакомить с нормативными документами и стандартами в области информационной безопасности.

#### *4. Изучение правовых и этических аспектов:*

- Ознакомить с законодательством РФ в области защиты персональных данных (Федеральный закон №152-ФЗ).
- Сформировать понимание этических норм поведения в сети Интернет.
- Ознакомить с ответственностью за нарушения в сфере информационной безопасности.

#### **Отличительные особенности программы**

Отличительными особенностями данной программы являются её практическая направленность на современные угрозы в сети Интернет, использование интерактивных методов обучения для максимального вовлечения учащихся, междисциплинарный подход, интегрирующий знания из различных областей, и акцент на формирование ответственности за свои действия в информационном пространстве.

**Уровень освоения программы** – ознакомительный.

**Объем программы:** 12 академических часов.

**Возраст обучающихся:** 14-16 лет.

**Наполняемость группы:** до 20 человек.

**Режим занятий:** 1 занятие 2 академических часа.

**Форма занятий:**

При реализации программы предусмотрено проведение различных по форме занятий, а именно:

- теоретические (лекции);
- практические (тренировочные, мастер-классы, проектная работа);
- комбинированные.

Формы организации обучения: индивидуальная работа, групповая работа, фронтальная работа.

#### **Ожидаемые результаты**

В результате освоения программы «Основы информационной безопасности» обучающиеся

*будут знать:*

- основные понятия информационной безопасности;
- наиболее распространенные угрозы в сети Интернет;
- основные правила безопасного поведения в сети Интернет и социальных сетях;
- основы защиты персональных данных;

*будут уметь:*

- разбираться в технологиях хранения данных;
- создавать надежные пароли;
- настраивать приватность в социальных сетях;
- применять основные правила безопасного поведения в сети Интернет

#### **Воспитательный потенциал программы**

Образовательный процесс программы заключается в формировании не только

знаний и навыков, но и нравственных качеств личности, ответственного отношения к информации и цифровым технологиям, а также активной гражданской позиции в информационном пространстве.

## 2. Содержание программы

### 2.1. Учебно-тематический план

| №<br>п/п | Название раздела/темы                                           | Количество часов |        |          | Формы<br>аттестации/<br>контроля |
|----------|-----------------------------------------------------------------|------------------|--------|----------|----------------------------------|
|          |                                                                 | всего            | теория | практика |                                  |
| 1.       | Основные понятия и определения ИБ                               | 2                | 2      | -        |                                  |
| 2.       | Категории и носители информации                                 | 2                | 1      | 1        | Практическая работа              |
| 3.       | Защита информации от несанкционированного доступа               | 2                | -      | 2        | Практическая работа              |
| 4.       | Угрозы информации. Методы и модели оценки уязвимости информации | 3                | 1      | 2        | Практическая работа              |
| 5.       | Средства защиты информации                                      | 3                | 1      | 2        | Практическая работа              |
| Итого:   |                                                                 | 12               | 5      | 7        |                                  |

### 2.2. Рабочая программа

#### 1. Основные понятия и определения ИБ (2 ч.)

*Теория:* Понятие информации и информационной безопасности.

#### 2. Категории и носители информации (2 ч.)

*Теория:* Изучить законодательный уровень информационной безопасности.

*Практика:* Законодательный уровень информационной безопасности.

#### 3. Защита информации от несанкционированного доступа (2 ч.)

*Практика:* Разработка комплексной системы защиты ИБ на примере предприятия.

#### 4. Угрозы информации. Методы и модели оценки уязвимости информации (3 ч.)

*Теория:* Узнаете какие бывают угрозы информации и методы уязвимости.

*Практика:* Групповая работа «Классификация угроз».

#### 5. Средства защиты информации (3 ч.)

*Теория:* Обзор основных средств защиты информации.

*Практика:* Создание итоговой презентации на основе выполненных работ.

### **3. Формы аттестации и оценочные материалы**

В процессе обучения будут применяться различные методы контроля, в том числе с использованием современных технологий.

*Текущий контроль.* Будет проводиться с целью непрерывного отслеживания уровня усвоения материала и стимулирования обучающихся. Для реализации текущего контроля в процессе объяснения теоретического материала педагог обращается к учащимся с вопросами и дает короткие задания.

*Тематический контроль.* Будет проводиться в виде практических заданий по итогам каждой темы с целью систематизации, обобщения и закрепления материала.

*Итоговая аттестация.* Проводится на основании выполненных работ.

#### **Оценочные материалы**

Практическая работа включает в себя задания, направленные на закрепление первичных знаний, формирование умений через выполнение заданий по образцу.

Устный опрос включает в себя систему вопросов, позволяющих выявить осознанность усвоения теоретической базы знаний, способность рассуждать, высказывать свое мнение, аргументировано строить ответ, активно участвовать в общей беседе, умение конкретизировать общие понятия.

Оценивание учебной деятельности слушателей и ее результатов при освоении программы осуществляется в баллах по всем видам контрольно-оценочных мероприятий (практическая работа/устный опрос/проектная работа).

### **4. Методическое обеспечение программы**

Методы обучения, используемые в программе: словесные, наглядные, практические, аналитические.

С целью стимулирования творческой активности слушателей будут использованы: метод проектов; методы сбора и обработки данных; исследовательский и проблемный методы; обобщение результатов.

Для обеспечения наглядности и доступности изучаемого материала будут использоваться: наглядные пособия смешанного типа (слайды, видеозаписи); дидактические пособия (карточки с заданиями, раздаточный материал).

### **5. Организационно-педагогические ресурсы**

#### **5.1 Специализированные лаборатории и классы, основные установки и стенды**

##### **Площадка:**

Мультимедийная аудитория, класс с соответствующим оборудованием.

#### **5.2 Оборудование и программное обеспечение:**

##### **Операционная система:**

Windows 7, Windows 8 и Windows 10 (Windows RT не поддерживается).

### **5.3 Аппаратное обеспечение:**

ПЭВМ по количеству учащихся (желательно ноутбук). Минимальные системные требования:

- операционная система Windows (XP, Vista, 7, 8) или MacOS (10.6, 10.7, 10.8);
- 4 ГБ оперативной памяти;
- процессор 2.5 ГГц;
- 8 ГБ свободного дискового пространства;
- разрешение экрана 1920\*1080.

### **5.4. Кадровое обеспечение программы**

#### **Реализаторы программы:**

Резниченко Ирина Владиславовна - инспектор по информационным системам отдела технического сопровождения и аналитики управления профессиональной навигации и приема НИТУ МИСИС.

## 6. Список литературы

### Нормативные документы:

1. Российская Федерация. Законы. Федеральный закон об образовании в Российской Федерации № 273-ФЗ [принят Государственной Думой от 12 декабря 2012 года : одобрен Советом Федерации 26 декабря 2012 года] – URL: <http://kremlin.ru/acts/bank/36698> (дата обращения: 29.07.2023).
2. Российская Федерация. Распоряжения. Распоряжение Правительства Российской Федерации № 678-р. Концепция развития дополнительного образования детей до 2030 года [утвержден распоряжением Правительства Российской Федерации от 31 марта 2022 года] – URL: <http://publication.pravo.gov.ru/Document/View/0001202204040022?ysclid=lkqp4xdhd1385635211&index=2> (дата обращения: 29.07.2023).
3. Российская Федерация. Приказы. Приказ об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным общеобразовательным программам № 629 [утвержден Министерством просвещения Российской Федерации 27 июля 2022 года] – URL: <http://publication.pravo.gov.ru/Document/View/0001202209270013?index=3> (дата обращения: 29.07.2023).
4. Российская Федерация. Постановления. Постановление об утверждении санитарных правил СП 2.4.3648-20 «Санитарно-эпидемиологические требования к организациям воспитания и обучения, отдыха и оздоровления детей и молодежи» [утверждены постановлением Главного государственного санитарного врача Российской Федерации 28 сентября 2020 года] – URL: [www.rospotrebnadzor.ru/files/news/SP2.4.3648-20\\_deti.pdf](http://www.rospotrebnadzor.ru/files/news/SP2.4.3648-20_deti.pdf) (дата обращения: 29.07.2023).

### Основная литература:

5. Вострецова Е.В. Основы информационной безопасности. - Екатеринбург: Урал, 2019. - 204 с.
6. Суворова Г.М. Информационная безопасность. - 2-е изд. - Москва: Юрайт, 2024. - 277 с.
7. Нестеров С.А. Основы информационной безопасности. - Санкт-Петербург: Лань, 2021. - 324 с.