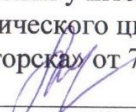



Муниципальное бюджетное общеобразовательное учреждение  
«Средняя общеобразовательная школа № 13 г. Лениногорска»  
муниципального образования «Лениногорский муниципальный район» Республики Татарстан

<p>«Рассмотрено» Протокол № 1 заседания методического объединения учителей естественно - математического цикла МБОУ «СОШ №13 г. Лениногорска» от 7 августа 2023 года  / <u>Ахметова Д.И.</u> подпись руководителя МО                      Ф.И.О.</p>	<p>«Согласовано» Заместитель директора по УВР МБОУ «СОШ №13 г. Лениногорска»  / <u>Шайдуллина Р.Г.</u> подпись    Ф.И.О. «14» августа 2023 г.</p>	<p>«Утверждено» Приказом №126 – ОД от 15.08.2023 г. «О внесении изменений в основную образовательную программу основного общего образования»</p>
---	---	--

## РАБОЧАЯ ПРОГРАММА

По учебному курсу «Информационная безопасность» основного общего образования 8-9 классов;

Период освоения рабочей программы: 2 года;

## I. Пояснительная записка

### **Общая характеристика учебного курса «Информационная безопасность»**

Программа курса внеурочной деятельности «Информационная безопасность» адресована учащимся 8-9 классов и направлена на достижение следующих планируемых результатов Федерального государственного образовательного стандарта основного общего образования:

- предметных (образовательные области «Математика и информатика», «Физическая культура, экология и ОБЖ»);
- метапредметных (регулятивных, познавательных, коммуникативных);
- личностных.

Курс является важной составляющей частью работы с учащимися, активно использующими различные сетевые формы общения (социальные сети, игры, пр.), задумывающимися о своей личной безопасности, безопасности своей семьи и своих друзей, а также проявляющими интерес к изучению истории и технологических основ информационной безопасности.

Программа курса ориентирована на выполнение требований к организации и содержанию урочной деятельности школьников. Ее реализация даёт возможность раскрытия индивидуальных способностей школьников, развития интереса к различным видам индивидуальной и групповой деятельности, закрепления умения самостоятельно организовать свою учебную, в том числе проектную деятельность. Кроме того, программа курса дает возможность закрепить ряд результатов обучения, предусмотренных программами учебных курсов по предметам «Информатика» и «Основы безопасности жизнедеятельности».

### **Цели и задачи изучения учебного курса «Информационная безопасность»**

**Главная цель курса** — обеспечить социальные аспекты информационной безопасности в воспитании школьников в условиях цифрового мира, включение цифровой гигиены в контекст воспитания детей на регулярной основе, формирование у выпускника школы правовой грамотности по вопросам информационной безопасности, которые влияют на социализацию детей в информационном обществе, формирование личностных и метапредметных результатов обучения и воспитания детей.

#### **Задачи курса по информационной безопасности детей:**

- формировать понимание сущности и воспитывать необходимость принятия обучающимися таких ценностей, как человеческая жизнь, свобода, равноправие и достоинство людей, здоровье, опыт гуманных, уважительных отношений с окружающими;
- создавать педагогические условия для формирования правовой и информационной культуры обучающихся, развития у них критического отношения к информации, ответственности за поведение в сети Интернет и по следствия деструктивных действий, формирования мотивации к познавательной, а не игровой деятельности, воспитания отказа от пустого времяпрепровождения в социальных сетях, осознания ценности живого человеческого общения;
- формировать отрицательное отношение ко всем проявлениям жестокости, насилия, нарушения прав личности, экстремизма во всех его формах в сети Интернет;
- мотивировать обучающихся к осознанному поведению на основе понимания и принятия ими морально-правовых регуляторов жизни общества и государства в условиях цифрового мира;
- научить молодых людей осознавать важность проектирования своей жизни и будущего своей страны — России в условиях развития цифрового мира, осознавать ценность ИКТ для достижения высоких требований к обучению профессиям будущего в мире, принимать средства Интернета как среду созидания, а не разрушения человека и общества.

Программа реализуется через следующие **формы занятий:**

- ситуационная игра;

- образно-ролевые игры;
- исследовательская деятельность;
- урок-практикум;
- дискуссия, обсуждение.

### Место учебного курса в учебном плане

Срок освоения рабочей программы: 8-9 классы, 2 года

Количество часов в учебном плане на изучение предмета (8-9 класс – 34 учебные недели)

Класс	Количество часов в неделю	Количество часов в год
8 класс	1	34
9 класс	1	34
Всего		68

### II. Содержание учебного курса «Информационная безопасность»

Содержание учебного курса «Информационная безопасность» для разных возрастных модулей программы складывается из двух линий:

- 1) Информационное общество и информационная культура.
- 2) Информационное пространство и правила информационной безопасности.

#### 8 класс.

*Линия «Информационное общество и информационная культура»*

Модуль 1. Информационное общество.

1.1. Информационное общество.

История создания сети Интернет.

Что такое Всемирная паутина?

1.2. Интернет как глобальная компьютерная сеть.

Как стать пользователем Интернета. Опасности для пользователей Интернета.

Сайты, электронные сервисы.

1.3. Угрозы в сети Интернет.

Защита личных данных в сети Интернет.

1.4. Сетевой этикет.

Коллекции сайтов для детей. Электронные музеи.

*Линия «Информационное пространство и правила информационной безопасности»*

Модуль 2. Правила пользователей сети Интернет.

2.1. Работа с СМС, электронной почтой, видеосервисами, в чатах и социальных сетях. Что такое информационная безопасность.

2.2. Защита от вредоносных программ и нежелательных рассылок, от негативных сообщений, защита своих устройств от внешнего вторжения.

2.3. Общение в социальной сети, работа с поисковыми системами и анализ информации, ответственность за распространение ложной и негативной информации, защита от нежелательных сообщений и контактов, вызов экстренной помощи.

2.4. Использование полезных ресурсов в сети Интернет, работа в сети Интернет для людей с особыми потребностями.

### **9 класс.**

#### *Линия «Информационное общество и информационная культура»*

Модуль 1. Современное информационное пространство и искусственный интеллект. 1.1. Киберпространство. Кибермиры. Киберфизическая система.

1.2. Киберобщество. Киберденьги. Кибермошенничество.

Модуль 2. Современная информационная культура.

2.1. Киберкультура. От книги к гипертексту. Киберкнига. Киберискусство.

2.2. Социальная инженерия. Классификация угроз социальной инженерии.

2.3. Новые профессии в киберобществе. Цифровизация профессий.

#### *Линия «Информационное пространство и правила информационной безопасности»*

Модуль 3. Угрозы информационной безопасности.

3.1. Киберугрозы. Кибервойны. Киберпреступность.

Уязвимости кибербезопасность.

Запрещенные и нежелательные сайты.

3.2. Защита от вредоносных программ и информационных атак.

3.3. Практика электронного обучения в сфере информационной безопасности.

### **III. Планируемые образовательные результаты учебного курса «Информационная безопасность»**

Программа учебного курса «Информационная безопасность» отражает в содержании цели поддержки и сопровождения безопасной работы с информацией в учебно-познавательной, творческой и досуговой деятельности (планируемые личностные, метапредметные и предметные результаты освоения курса).

В соответствии с федеральным государственным образовательным стандартом основного общего образования необходимо сформировать у обучающихся с учетом возрастных особенностей на каждом уровне общего образования такие *личностные результаты*, которые позволят им грамотно ориентироваться в информационном мире с учетом имеющихся в нем угроз:

- принимать ценности человеческой жизни, семьи, гражданского общества, многонационального российского народа, человечества;
- быть социально активными, уважающими закон и правопорядок, соизмеряющими свои поступки с нравственными ценностями, осознающими свои обязанности перед семьей, обществом, Отечеством;
- уважать других людей, уметь вести конструктивный диалог, достигать взаимопонимания, сотрудничать для достижения общих результатов;
- осознанно выполнять правила здорового образа жизни, безопасного для человека и окружающей его среды.

В рамках достижения этих личностных результатов при реализации программы курса информационной безопасности наиболее актуально в условиях быстро меняющегося и несущего в себе угрозы информационного мира обеспечить:

- развитие морального сознания и компетентности в решении моральных проблем на основе личного выбора, формирование нравственных чувств и нравственного поведения, осознанного и ответственного отношения к собственным поступкам;
- формирование ценности здорового и безопасного образа жизни; усвоение правил индивидуального и коллективного безопасного поведения в чрезвычайных ситуациях, угрожающих жизни и здоровью людей.

В результате освоения программы курса информационной безопасности акцентируется внимание на *метапредметных результатах* освоения основной образовательной программы:

- освоение социальных норм, правил поведения, ролей и форм социальной жизни в группах и сообществах, включая взрослые и социальные сообщества; участие в школьном самоуправлении и общественной жизни в пределах возрастных компетенций с учетом региональных, этнокультурных, социальных и экономических особенностей;
- формирование коммуникативной компетентности в общении и сотрудничестве со сверстниками, детьми старшего и младшего возраста, взрослыми в процессе образовательной, общественно полезной, учебно-исследовательской, творческой и других видов деятельности;
- умение использовать средства информационно-коммуникационных технологий (ИКТ) в решении когнитивных, коммуникативных и организационных задач с соблюдением требований эргономики, техники безопасности, гигиены, ресурсосбережения, правовых и этических норм, норм информационной безопасности.

Планируется достижение *предметных результатов*, актуальных для курса информационной безопасности в интеграции с предметами «Информатика» и (или) «ОБЖ».

*Линия «Информационное общество и информационная культура»:*

- понимание личной и общественной значимости современной культуры безопасности жизнедеятельности;
- знание основных опасных и чрезвычайных ситуаций социального характера, включая экстремизм и терроризм, и их последствий для личности, общества и государства; формирование антиэкстремистской и антитеррористической личностной позиции;
- знание и умение применять меры безопасности и правила поведения в условиях опасных и чрезвычайных ситуаций.

*Линия «Информационное пространство и правила информационной безопасности»:*

- формирование навыков и умений безопасного и целесообразного поведения при работе с компьютерными программами и в Интернете, умения соблюдать нормы информационной этики;
- умение принимать обоснованные решения в конкретной опасной ситуации с учетом реально складывающейся обстановки и индивидуальных возможностей.

В результате освоения программы курса с учетом возрастных групп выпускник освоит жизненно важные практические компетенции.

*Выпускник научится понимать:*

- источники информационных угроз, вредоносные программы и нежелательные рассылки, поступающие на мобильный телефон, планшет, компьютер;
- роль близких людей, семьи, правоохранительных органов для устранения проблем и угроз в сети Интернет и мобильной телефонной связи, телефоны экстренных служб;
- виды информационных угроз, правила поведения для защиты от угроз, виды правовой ответственности за проступки и преступления в сфере информационной безопасности;
- проблемные ситуации и опасности в сетевом взаимодействии и правила поведения в проблемных ситуациях, ситуациях профилактики и предотвращения опасности;
- этикет сетевого взаимодействия, правовые нормы в сфере информационной безопасности;
- правила защиты персональных данных;
- назначение различных позитивных ресурсов в сети Интернет для образования и в профессиях будущего.

*Выпускник научится применять на практике:*

- правила цифровой гигиены для использования средств защиты персональных данных (формировать и использовать пароль, использовать код защиты персонального устройства, регистрироваться на сайтах без распространения личных данных);
- компетенции медиаинформационной грамотности при работе с информацией в сети Интернет, критическое и избирательное отношение к

источникам информации;

— компетенции компьютерной грамотности по защите персональных устройств от вредоносных программ, использованию антивирусных программных средств, лицензионного программного обеспечения;

— информационно-коммуникативные компетенции по соблюдению этических и правовых норм взаимодействия в социальной сети или в мессенджере, умение правильно вести себя в проблемной ситуации (оскорбления, угрозы, предложения, агрессия, вымогательство, ложная информация и др.), отключаться от нежелательных контактов, действовать согласно правовым нормам в сфере информационной безопасности (защиты информации).

*Выпускник освоит нормы культуры информационной безопасности в системе универсальных учебных действий для самостоятельного использования в учебно-познавательной и досуговой деятельности позитивного Интернета и средств электронного обучения с соблюдением правил информационной безопасности.*

Для выявления достижения планируемых результатов обучения рекомендуется использовать диагностические тесты и опросы, проектные работы и конкурсы по информационной безопасности в образовательных организациях.

#### IV. Тематическое планирование учебного курса «Информационная безопасность» 8 КЛАСС (34 ЧАСА)

Раздел (тема), кол-во часов	Основное содержание	Номер и тема урока	Методы и формы организации обучения. Основные виды деятельности обучающихся	Электронные (цифровые) образовательные ресурсы
<b>Раздел 1. Что нужно знать?</b>	<i>Линия «Информационное общество и информационная культура»</i> Модуль 1. Информационное общество. Информационное общество. История создания сети Интернет. Что такое Всемирная паутина? Интернет как глобальная компьютерная сеть. Как стать пользователем Интернета. Опасности для пользователей Интернета. Сайты, электронные сервисы. Угрозы в сети Интернет. Защита личных данных в сети Интернет. Сетевой этикет. Коллекции сайтов для детей. Электронные музеи.	1) Что такое информационное общество 2) Пространство Интернета на Земле. 3) История создания сети Интернет 4) Что такое Всемирная паутина. 5-6) Путешествие по сети интернет: сайты и электронные сервисы. 7) Как стать пользователем Интернета 8-9) Опасности для пользователей Интернета 10) Что такое кибератака. 11) Что такое информационная	Словесные и наглядные методы при изложении материала  Практические методы. Практические работы	<a href="https://xn----7sbbfb7a7aej.xn--p1ai/informatika_09_34_sim">https://xn----7sbbfb7a7aej.xn--p1ai/informatika_09_34_sim</a>

		<p>безопасность  12-13) Законы о защите  личных данных в Интернете  14) Сетевой этикет  15) Коллекция сайтов для  детей  16-18) Электронные музеи</p>		
<p><b>Раздел2.  Что нужно  уметь?</b></p>	<p><i>Линия «Информационное  пространство и правила  информационной безопасности»</i>  Модуль 2. Правила пользователей  сети Интернет. Работа с СМС,  электронной почтой, видеосервисами,  в чатах и социальных сетях. Что такое  информационная безопасность.  Защита от вредоносных программ и  нежелательных рассылок, от  негативных сообщений, защита своих  устройств от внешнего вторжения.  Общение в социальной сети, работа с  поисковыми системами и анализ  информации, ответственность за  распространение ложной и  негативной информации, защита от  нежелательных сообщений и  контактов, вызов экстренной помощи.  Использование полезных ресурсов в  сети Интернет, работа в сети  Интернет для людей с особыми  потребностями.</p>	<p>19) Правила работы с СМС  20-21) Правила работы с  электронной почтой  22) Правила работы с  видеосерверами  23) Правила работы в  социальных сетях  24) Правила защиты от  вирусов, спама, рекламы и  рассылок  25) Правила защиты от  негативных сообщений  26) Правила общения в  социальной сети  27) Правила работы с  поисковыми системами и  анализ информации  28) Правила  ответственности за  распространение ложной и  негативной информации  29) Правила защиты от  нежелательных сообщений  и контактов  30) Правила вызова  экстренной помощи  31) Правила защиты</p>	<p>Практические методы.  Практические работы</p>	<p><a href="https://xn----7sbbfb7a7aej.xn--p1ai/informatika_09_34_sim">https://xn----7sbbfb7a7aej.xn--p1ai/informatika_09_34_sim</a></p>

		устройств от внешнего вторжения 32) правила выбора полезных ресурсов в Интернете 33) Средства работы в Интернете для людей с особыми потребностями. 34) Обобщающий урок. Зачет.		
--	--	--	--	--

**9 КЛАСС (34 часа)**

Раздел (тема), кол-во часов	Основное содержание	Номер и тема урока	Методы и формы организации обучения. Основные виды деятельности обучающихся	Электронные (цифровые) образовательные ресурсы
<b>Раздел 1. Киберпространство</b>	<i>Линия «Информационное общество и информационная культура»</i> Модуль 1. Современное информационное пространство и искусственный интеллект. Киберпространство. Кибермиры. Киберфизическая система. Киберобщество. Киберденьги. Кибермошенничество.	1) Киберпространство 2) Кибермиры 3) Киберфизическая система 4) Киберобщество 5) Киберденьги 6) Кибермошенничество 7-10) Практикум по 1 разделу Практическая работа на основе онлайн курса Академии Яндекса «Безопасность в Интернете» по теме «Безопасные платежи» 11) Контрольное занятие/ тестирование	Словесные и наглядные методы при изложении материала  Практические методы. Практические работы	<a href="https://xn----7sbbfb7a7aej.xn--p1ai/informatika_09_34_sim">https://xn----7sbbfb7a7aej.xn--p1ai/informatika_09_34_sim</a>



<p><b>Раздел 2. Киберкультура</b></p>	<p>Модуль 2. Современная информационная культура. Киберкультура. От книги к гипертексту. Киберкнига. Киберискусство. Социальная инженерия. Классификация угроз социальной инженерии. Новые профессии в киберобществе. Цифровизация профессий.</p>	<p>12) Киберкультура 13) От книги к гипертексту 14) Кибернига 15) Киберискусство 16) Социальная инженерия 17) Классификация угроз социальной инженерии 18-22) Практикум к разделу 2. Практическая работа от компаний мобильной связи 23) Контрольное занятие/ тестирование</p>	<p>Словесные и наглядные методы при изложении материала</p> <p>Практические методы. Практические работы</p>	<p><a href="https://xn----7sbbfb7a7aej.xn--p1ai/informatika_09_34_sim">https://xn----7sbbfb7a7aej.xn--p1ai/informatika_09_34_sim</a></p>
<p><b>Раздел 3. Киберугрозы</b></p>	<p><i>Линия «Информационное пространство и правила информационной безопасности»</i> Модуль 3. Угрозы информационной безопасности. Киберугрозы. Кибервойны. Киберпреступность. Уязвимости кибербезопасность. Запрещенные и нежелательные сайты. Защита от вредоносных программ и информационных атак. Практика электронного обучения в сфере информационной безопасности.</p>	<p>24) Кибервойны 25) Киберпреступность 26) Примеры киберпреступности 27) Уязвимости кибероопасности 28) Угрозы информационной безопасности 29) Запрещенные и нежелательные сайты 30-33) Практикум к разделу 3 Практическая работа на основе онлайн курса Академии Яндекса «Безопасность в интернете» по темам: защита вредоносных программ; безопасность аккунтов. 34) Обобщающий урок. Зачет.</p>	<p>Словесные и наглядные методы при изложении материала</p> <p>Практические методы. Практические работы</p>	<p><a href="https://xn----7sbbfb7a7aej.xn--p1ai/informatika_09_34_sim">https://xn----7sbbfb7a7aej.xn--p1ai/informatika_09_34_sim</a></p>