МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Министерство образования и науки Алтайского края
Комитет по образованию г. Барнаула
МБОУ "Гимназия №74"

РАССМОТРЕНО	СОГЛАСОВАНО	УТВЕРЖДЕНО
Руководитель МО	Зам.директора по УР	Директор МБОУ «Гимназия №74»
_____ / О.П.Кривощапова	_____ / О.В.Слободянник	_____ Т. В. Евдокимова
Протокол № 1		Приказ № 303-осн
от 29.08.2024 г.	29.08.2024 г.	от 29.08.2024 г.

Рабочая программа
учебного курса
«Информационная безопасность»
для 8 классов
на 2024/2025 учебный год

.

Барнаул – 2024 г.

Пояснительная записка

Рабочая программа учебного курса «Информационная безопасность» для 8 классов составлена в соответствии с требованиями обновлённого Федерального государственного образовательного стандарта основного общего образования (ФГОС ООО) и с учётом Примерной образовательной программы учебного курса «Информационная безопасность» для образовательных организаций, реализующих образовательные программы основного общего образования, одобренной решением федерального учебно-методического объединения по общему образованию (протокол от 26 октября 2020 № 4/20).

ЦЕЛИ ИЗУЧЕНИЯ УЧЕБНОГО КУРСА «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

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

— формировать понимание сущности и воспитывать необходимость принятия обучающимися таких ценностей, как ценность человеческой жизни, свободы, равноправия и достоинства людей, здоровья, опыта 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 последствия 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, ценность ИКТ для достижения высоких требований к обучению профессиям будущего в мире, принимать средства в Интернете как среду созидания, а не разрушения человека и общества.

МЕСТО УЧЕБНОГО ПРЕДМЕТА «ИНФОРМАТИКА» В УЧЕБНОМ ПЛАНЕ.

Учебным планом на изучение учебного курса «Информационная безопасность» в 8 классе на базовом уровне отведено 34 учебных часа — по 1 часу в неделю.

Содержание учебного предмета

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.

Планируемые результаты освоения учебного курса

ЛИЧНОСТНЫЕ РЕЗУЛЬТАТЫ

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 личностного 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.

МЕТАПРЕДМЕТНЫЕ РЕЗУЛЬТАТЫ

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.

ПРЕДМЕТНЫЕ РЕЗУЛЬТАТЫ

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.

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.

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).

Тематическое планирование

№ п/п	Наименование разделов / тем программы	Количество часов	Электронные (цифровые) образовательные ресурсы
1.	Модуль 1. Современное информационное пространство и искусственный интеллект	10	1) РЭШ – Российская электронная школа: https://resh.edu.ru/ 2) Единая коллекция цифровых образовательных ресурсов: http://school-collection.edu.ru/ 3) Учительский портал: http://www.uchportal.ru/ 4) Видеоуроки по основным предметам школьной программы: http://inerneturok.ru/
2.	Модуль 2. Современная информационная культура	10	
3.	Модуль 3. Угрозы информационной безопасности	10	
4.	Заключительное повторение изученного.	4	
ОБЩЕЕ КОЛИЧЕСТВО ЧАСОВ ПО ПРОГРАММЕ		**34**	

Поурочное тематическое планирование

№ урока	Наименование темы	Дата проведения	Корректировка
1.	1.1. Киберпространство. Кибермиры. Киберфизическая система		

2.	1.1. Киберпространство. Кибермиры. Киберфизическая система		
3.	1.1. Киберпространство. Кибермиры. Киберфизическая система		
4.	1.1. Киберпространство. Кибермиры. Киберфизическая система		
5.	1.1. Киберпространство. Кибермиры. Киберфизическая система		
6.	1.2. Кибероббщество. Киберденьги. Кибермошенничество		
7.	1.2. Кибероббщество. Киберденьги. Кибермошенничество		
8.	1.2. Кибероббщество. Киберденьги. Кибермошенничество		
9.	1.2. Кибероббщество. Киберденьги. Кибермошенничество		
10.	1.2. Кибероббщество. Киберденьги. Кибермошенничество		
11.	2.1. Киберкультура. От книги к гипертексту. Киберкнига. Киберискусство.		
12.	2.1. Киберкультура. От книги к гипертексту. Киберкнига. Киберискусство.		
13.	2.1. Киберкультура. От книги к гипертексту. Киберкнига. Киберискусство.		
14.	2.1. Киберкультура. От книги к гипертексту. Киберкнига. Киберискусство.		
15.	2.2. Социальная инженерия. Классификация угроз социальной инженерии		
16.	2.2. Социальная инженерия. Классификация угроз социальной инженерии		
17.	2.2. Социальная инженерия. Классификация угроз социальной инженерии		
18.	2.2. Социальная инженерия. Классификация угроз социальной инженерии		
19.	2.3. Новые профессии в кибероббществе. Цифровизация профессий		
20.	2.3. Новые профессии в кибероббществе. Цифровизация профессий		
21.	3.1. Киберугрозы. Кибервойны. Киберпреступность. Уязвимости кибербезопасности. Угрозы информационной безопасности. Запрещенные и нежелательные сайты		
22.	3.1. Киберугрозы. Кибервойны. Киберпреступность. Уязвимости кибербезопасности. Угрозы информационной безопасности. Запрещенные и нежелательные сайты		

23.	3.1. Киберугрозы. Кибервойны. Киберпреступность. Уязвимости кибербезопасности. Угрозы информационной безопасности. Запрещенные и нежелательные сайты		
24.	3.1. Киберугрозы. Кибервойны. Киберпреступность. Уязвимости кибербезопасности. Угрозы информационной безопасности. Запрещенные и нежелательные сайты		
25.	3.2. Защита от вредоносных программ и информационных атак		
26.	3.2. Защита от вредоносных программ и информационных атак		
27.	3.2. Защита от вредоносных программ и информационных атак		
28.	3.3. Практика электронного обучения в сфере информационной безопасности		
29.	3.3. Практика электронного обучения в сфере информационной безопасности		
30.	3.3. Практика электронного обучения в сфере информационной безопасности		
31.	Повторение		
32.	Повторение		
33.	Повторение		
34.	Повторение		