Комитет по образованию Администрации Черлакского муниципального района

Муниципальное бюджетное общеобразовательное учреждение
«Иртышская средняя общеобразовательная школа»
Черлакского муниципального района

РАССМОТРЕНО	СОГЛАСОВАНО	УТВЕРЖДЕНО
на заседании Педагогического Совета МБОУ "Иртышская СОШ"	Заместитель директора по УВР МБОУ "Иртышская СОШ" _____ Куратова С.С.	Директор школы _____ Беляева Ф.Н. Приказ №73/2 от «30» августа 2024 г.

Дополнительная общеобразовательная общеразвивающая программа (модульная) технической направленности «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Возраст обучающихся - 8 - 17 лет
Срок реализации - 1 год (144 часа)
Очная форма освоения
Базовый уровень сложности

Составитель:
педагог дополнительного образования
Тимофеева А. Ю.

с. Иртыш, 2024 г.

СОДЕРЖАНИЕ

1. Пояснительная записка

Данная программа составлена на основе следующих нормативных документов: Федеральный Закон от 29.12.2012 № 273-ФЗ «Об образовании в РФ», Концепция развития дополнительного образования детей (Распоряжение Правительства РФ от 4 сентября 2014 г. № 1726-р), Постановление Главного государственного санитарного врача РФ от 04.07.2014 № 41 «Об утверждении СанПиН 2.4.4.3172-14 «Санитарно-эпидемиологические требования к устройству, содержанию и организации режима работы образовательных организаций дополнительного образования детей», Приказ Министерства образования и науки Российской Федерации (Минобрнауки России) от 9 ноября 2018 г. № 196 г. Москва «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным общеобразовательным программам», авторской программы «Иформационная безопасность», автор Цветкова, М. С. Информационная безопасность. 2-11 классы : методическое пособие / М. С. Цветкова. – М.: БИНОМ. Лаборатория знаний.

Программа ориентирована на проведение занятий по информационной безопасности школьников и безопасному поведению в сети Интернет и отражает актуальные вопросы безопасной работы с персональной информацией, сообщениями и звонками по мобильному телефону, электронной почтой, информационными и коммуникационными ресурсами в сети Интернет, доступа к ресурсам для досуга, поиска новостной, познавательной, учебной информации, общения в со-циальных сетях, получения и передачи файлов, размещения личной информации в коллективных социальных серви-сах. В основе курса лежат технические, этические и правовые нормы соблюдения информационной безопасности, установленные контролирующими и правоохранительными органами, а также практические рекомендации ведущих ИТ-компаний и операторов мобильной связи Российской Федерации.

При реализации требований безопасности в сети Интернет для любого пользователя, будь это школьник или учитель, образовательное учреждение должно обеспечивать защиту конфиденциальных сведений,

представляющих собой, в том числе, персональные данные школьника. Но включение детей в интернет-взаимодействие наиболее активно осуществляется вне школы без надлежащего надзора со стороны взрослых.

В связи с этим в настоящее время необходимо особое внимание уделять воспитанию у детей культуры информационной безопасности при работе в сети Интернет вне школы. Для этого необходимо проводить непрерывную образовательно-просветительскую работу с детьми, начиная с младшего школьного возраста, формировать у родителей и учащихся ответственное и критическое отношение к источникам негативной информации, в том числе внимательно относиться к использованию детьми личных устройств мобильной связи, домашнего компьютера с Интернетом, телевизора, подключенного к Интернету, использовать дома программные средства защиты от доступа детей к негатив-ной информации или информации по возрастным признакам (возраст+). Научить школьника правильно ориентироваться в большом количестве ресурсов в сети Интернет является важной задачей для вовлечения детей в современную цифровую образовательную среду, отвлечения их от бесполезного, отвлекающего контента, бесцельной траты времени в соци-альных сетях и мессенджерах.

Главная цель — обеспечение социальных аспектов информационной безопасности в воспитании школьников в условиях цифрового мира, включение цифровой гигиены в контекст воспитания детей на регулярной основе, формиро-вание у выпускника школы правовой грамотности по вопро-сам информационной безопасности, которые влияют на соци-ализацию детей в информационном обществе, формирование личностных и метапредметных результатов обучения и воспитания детей.

Задачи :

- сформировать понимание сущности и воспитывать необходимость принятия обучающимися таких ценностей, как человеческая жизнь, свобода, равноправие и достоинство людей, здоровье, опыт гуманных, уважительных отношений с окружающими;
- создать педагогические условия для формирования правовой и информационной культуры обучающихся, развития у них критического отношения к информации, ответственности за поведение в сети Интернет и последствий деструктивных действий, формирования мотивации к познавательной, а не игровой деятельности, воспитания отказа от пустого времяпрепровождения в социальных сетях, осознания ценности живого человеческого общения;
- сформировать 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 усло-виях цифрового мира;
- научить молодых людей осознавать важность проек-тирования 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 в Интернете как среду созидания, а не разру-шения человека и общества.

Планируемые результаты:

Личностные результаты:

В соответствии с ФГОС общего образования необходимо сформировать у учащихся такие личностные результаты, которые позволят подростку ориентироваться в информационном мире с учетом имеющихся в нем угроз:

- Принимать ценности человеческой жизни, семьи, граж-данского общества, многонационального российского на-рода, человечества.
- Быть социально активным, уважающим закон и право-порядок, соизмеряющим свои поступки с нравственными ценностями, осознающим свои обязанности перед семьей, обществом, Отечеством.
- Уважать других людей, уметь вести конструктивный диалог, достигать взаимопонимания, сотрудничать для достижения общих результатов.
- Осознанно выполнять правила здорового и экологически целесообразного образа жизни, безопасного для человека и окружающей его среды.

Метапредметные результаты:

В результате обучения по модулям курса акцентируется внимание на такие метапредметные результаты освоения основной образовательной программы основного общего образования, как:

- 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 региональсо сверстниками, детьми старшего и младшего возраста, взрослыми в процессе образовательнных, этнокультурных, социальных и экономических особенностей;
- формирование коммуникативной компетентности в общении и сотрудничестве ой, общественно полезной, учебно-исследовательской, творческой и других видов деятельности;

- умение использовать средства информационных и коммуникационных технологий (далее — 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 (общие):

Также планируется достижение некоторых предметных результатов, актуальных для данного курса в интеграции с предметами: «Окружающий мир» для 2-4 классов, «Информатика» и ОБЖ для 5-6 и 7-9 классов, «Обществознание» и «Информатика» (раздел «Социальная информатика») для 10-11 классов, например:

- формирование основ правосознания для соотнесения собственного поведения и поступков других людей с нравственными ценностями и нормами поведения, установленными законодательством Российской Федерации;
- освоение приемов работы с социально значимой информацией, ее осмысление; развитие способностей обучающихся делать необходимые выводы и давать обоснованные оценки социальным событиям и процессам;
- формирование навыков и умений безопасного и целесообразного поведения при работе с компьютерными программами и в Интернете, умения соблюдать нормы информационной этики и права.

Планируется достижение некоторых предметных результа-тов, актуальных для данного курса в предметах.

В результате освоения курса учащиеся будут

знать и понимать:

- источники угроз, поступающих на мобильный телефон, планшет, компьютер
- виды угроз
- проблемные ситуации в сетевом взаимодействии
- правила поведения для защиты от угроз
- правила поведения в проблемных ситуациях
- этикет сетевого взаимодействия
- роль близких людей, семьи для устранения проблем и угроз в сети Интернет и мобильной телефонной связи
- телефоны экстренных служб
- личные данные

позитивный Интернет

Уметь:

- правильно использовать аватар с учетом защиты личных данных
- формировать и использовать пароль
- использовать код защиты телефона
- регистрироваться на сайтах без распространения личных данных
- вести общение в социальной сети или в мессенджере сообщений
- правильно вести себя в проблемной ситуации (оскорбления, угрозы, предложения, агрессия, вымогательство, ложная информация и др.)
- отключиться от нежелательных контактов
- использовать позитивный Интернет.

2. Учебно-тематическое планирование (2-4 класс)

Курс 2-4 класс	Тема занятия	Теория	Практика	Всего
	Модуль 1. Правила безопасной работы в сети Интернет с мобильным телефоном.	**4**	**9**	**13**
1.	Введение. Уроки Смайлика	1	1	2
2.	СМС от неизвестных лиц. Звонки с предложениями. Защита от входа в твой телефонЛожные сообщения. Угрозы в СМС	1	4	5
3.	Подключение телефона к «Вай-Фай» сети. Вызов экстренных служб. Телефонное хулиганство	1	3	4
4.	Итоговое занятие. Викторина «Правила безопасности в сети на телефоне»	1	1	2
	Модуль 2. Правила безопасной работы в сети Интернет	**1**	**6**	**7**

	с планшетом или на компьютере			
1	Мой планшет или компьютер: защита входа		1	1
2	Моя почта, логин и пароль. Спам. Почта от неизвестных лиц. Вирусы	1	3	4
3	Регистрация на сайтах: личные данные		1	1
4	Итоговое занятие. Викторина «Правила безопасности в сети на компьютере»		1	1
	Модуль 3. Путешествуем в сети Интернет	**3**	**6**	**9**
1	Поиск информации в Интернете	1	1	2
2	Сайты для детей. Сайты о безопасном поведении. Сайты для учебы	1	1	2
3	Сайты с электронными книгами. Сайты с коллекциями для детей	1	1	2
4	Итоговое занятие. Викторина «Цифровая гигиена»		2	2
	Модуль 4. Правила безопасной работы в социальной сети	**1**	**6**	**7**
	Социальные сети для детей Что такое Аватар и как его выбрать. «Друг» в сети, кто за ним прячется	1	1	2
	Ложные сообщения. Что говорить о себе незнакомцам Спроси совета в семье		1	1
	Этикет в общении. Нельзя обижать. Если тебя обижают		1	1
	Защити себя от не-доброжелателей. Если тебе угрожают. Агрессия и грубость		1	1
	Уговоры и предложения. Отключение от не-желательных контактов		1	1
	Итоговое занятие. Конкурс рисунков «Правила поведения в сети Интернет»		1	1
Всего за курс:		**9**	**27**	**36**

Учебно-тематическое планирование (5-6 класс)

Курс 2-4 класс	**Тема занятия**	**Теория**	**Практика**	**Всего**
	Модуль 1. Что нужно знать? Пространство Интернета на планете Земля	**6**	**12**	**18**
1.	История создания сети Интернет. Что такое Всемирная паутина	1	1	2
2.	Путешествие по сети Интернет: сайты и электронные сервисы	1	2	3
3.	Как стать пользователем Интернета. Опасности для пользователей Интернета	1	2	3
4.	Что такое кибератака. Что такое информационная безопасность	2	1	3
5.	Законы о защите личных данных в Интернете. Сетевой этикет	1	2	3
6.	Коллекции сайтов для детей. Электронные музеи		3	3
7.	Итоговое занятие. Конкурс рисунков «Правила поведения в сети Интернет»		1	1
	Модуль 2. Что нужно уметь? Правила для пользователей сети Интернет	**5**	**13**	**18**
1	Правила работы с СМС		1	1

2	Правила работы с электронной почтой, видеосервисами, в социальных сетях	1	2	3
3	Правила защиты от вирусов, спама, рекламы и рассылок, негативных сообщений	1	2	3
4	Правила общения в социальной сети		1	1
5	Правила работы с поисковыми системами и анализ информации. Правила защиты от нежелательных сообщений и контактов	1	1	2
6	Правила ответственности за распространение ложной и негативной информации	1	1	2
7	Правила вызова экстренной помощи. Правила защиты устройств от внешнего вторжения		2	2
8	Правила выбора полезных ресурсов в Интернете		1	1
9	Средства работы в Интернете для людей с особыми потребностями	1	1	2
10	Итоговое занятие.Конкурс кроссвордов — презентаций «Цифровая гигиена»		1	1
Всего за курс:		**11**	**25**	**36**

Учебно-тематическое планирование (7-9 класс)

Курс 2-4 класс	**Тема занятия**	**Теория**	**Практика**	**Всего**
	Модуль «Киберпространство»	**4**	**9**	**13**
1.	Киберпространство. Кибермиры. Киберфизическая система. Кибероббщество. Киберденьги. Кибермошенничество	4	4	8
2.	Практическая работа на основе онлайн- курса Академии Яндекс «Безопасность в Интернете» по теме «Безопасные онлайн-платежи ».		4	4
3.	Итоговое занятие. Тест к модулю 1.		1	1
	Модуль «Киберкультура»	**4**	**8**	**12**
1	Киберкультура. От книги к гипертексту. Киберкнига. Киберискусство. Социальная инженерия. Классификация угроз социальной инженерии	4	4	8
2	Практическая работа от компаний мобильной связи Билайн, МТС и Мегафон (по выбору учащихся)		3	3
3	Итоговое занятие.Тест к модулю 2		1	1
	Модуль «Киберугрозы»	**2**	**9**	**11**
1	Кибервойны. Киберпреступность. Примеры киберпреступлений. Уязвимости кибербезопасности. Угрозы информационной безопасности. Запрещенные и нежелательные сайты. Новые профессии в кибероббществе	2	5	7
2	Практическая работа на основе онлайн- курса Академии Яндекса «Безопасность в Интернете» (продолжение), по темам: защита от вредоносных программ; безопасность аккаунтов		3	3
3	Итоговое занятие.Тест к модулю 3		1	1

Всего за курс:		**10**	**26**	**36**

Учебно-тематическое планирование (10-11 класс)

Курс 2-4 класс	**Тема занятия**	**Теория**	**Практика**	**Всего**
	Модуль 1. Правовые основы информационной безопасности	**2**	**3**	**5**
1.	Основные документы в области информационной безопасности Российской Федерации Субъективная и объективная стороны юридической ответственности	1	1	2
2.	Информация как объект правовых от-ношений. Функции, принципы и виды юридиче-ской ответственности	1	1	2
3.	.Итоговое занятие. Подготовка презентации по теме в группах учащихся		1	1
	Модуль 2. Законодатель-ство Российской Федера-ции о гражданско-право-вой ответственности в сфере инфобезопасности	**3**	**5**	**8**
1	Законодательство Российской Федерации о гражданско-правовой ответственности	1	2	3
2	Гражданско-правовая ответственность несовер-шеннолетних за проступки в области информационной безопасности (защиты информации)	2	2	4
3	Итоговое занятие.Тест к модулю 2		1	1
	Модуль 3. **Законодатель-ство Российской Федера-ции об административной ответственности в сфере инфобезопасности**	**4**	**8**	**12**
1	Понятие административной ответственности	1	1	2
2	Административная ответственность несовершеннолетних граждан за проступки в области информационной безопасности (защиты информации).	1	2	3
3	Ответственность за проступок в области нарушения авторских прав на лицензион-ное программное обеспечение	1	2	3
4	Ответственность за проступок — за оскорбления, в том числе в социальных сетях	1	2	3
5	Итоговое занятие.Тест к модулю 3		1	1
	М**одуль 4. Законода-тельство Российской Федерации об уголовной ответственности в сфере инфобезопасности**	**3**	**8**	**11**
1	Понятие уголовной ответственности	1		1
2	Уголовная ответст-венность несовершеннолетних за преступления в области информационной безопасности (защиты информации)	2	4	6
3	Итоговое занятие. Подготовка и защита проекта по теме.		4	4
Всего за курс:		**12**	**24**	**36**

3. Содержание курса (2-4 класс)
(36 часов)

Модуль 1. Правила безопасной работы в сети Интернет с мобильным телефоном. (13 ч.)

Теория. Уроки Смайлика. Угрозы из СМС сообщений. Угрозы от незнакомых лиц.

Практика. Ложные сообщения и просьбы. Проблемы хулиганства по телефону. Телефоны экстренных служб. Выход в Интернет, беспроводную сеть. Защита устройства от входа, код входа.

Модуль 2. Правила безопасной работы в сети Интернет с планшетом или на компьютере. (7 ч.)

Теория. Защита входа в устройство. Пароль и логин.

Практика. Электронная почта. Спам. Вирусы. Регистрация на сайтах. Личные дан-ные.

Модуль 3. Путешествуем в сети Интернет. (9 ч.)

Теория. Поиск информации в сети Интернет. Позитивный Интернет.

Практика.Сайты для учебы, досуга, творчества, чтения книг, виртуальных путешествий.

Модуль 4. Правила безопасной работы в социальной сети. (7 ч.)

Теория.Этикет общения. Реакция на негативные сообщения, угрозы, агрессию, уговоры и опасные предложения. Отключение от нежелательных контактов

Практика.Социальные сети. Детские социальные сети. Аватар и его выбор. «Друзья» в сети. Опасности общения в социальной сети с виртуальными «друзьями». Поддержка семьи для устранения проблем общения в социальных сетях.

Содержание курса (5-6 класс)
(36 часов)

Модуль 1. Что нужно знать? Пространство Интернета на планете Земля (18 ч.)

Теория. История создания сети Интернет. Что такое Всемирная паутина? Путешествие по сети Интернет: сайты и электронные сервисы. Как стать пользователем Интернета?

Практика. Опасности для пользователей Интернета. Что такое кибератака. Что такое информационная безопасность. Законы о защите личных данных в Интернете. Сетевой этикет. Коллекции сайтов для детей. Электронные музеи.

Модуль 2. Что нужно уметь? Правила для пользователей сети Интернет (18 ч.)

Теория. Правила работы с СМС. Правила работы с электронной почтой. Правила работы с видеосервисами. Правила работы в социальных сетях. Правила защиты от вирусов, спама, рекламы и рассылок. Правила защиты от негативных сообщений.

Практика. Правила общения в социальной сети. Правила работы с поисковыми системами и анализ информации. Правила ответственности за распространение ложной и негативной информации. Правила защиты от нежелательных сообщений и контактов. Правила вызова экстренной помощи. Правила защиты устройств от внешнего вторжения. Правила выбора полезных ресурсов в Интернете. Средства работы в Интернете для людей с особыми потребностями

Содержание курса (7-9 класс)
(36 часов)

Модуль 1. Киберпространство. (13 часов)

Теория. Киберпространство. Кибермиры. Киберфизическая систе-ма. Киберобщество. Киберденьги. Кибермошенничество.

Практика. Практикум к разделу 1. Практическая работа на основе он- лайн курса Академии Яндекс «Безопасность в Интернете» по теме «Безопасные онлайн-платежи».

Тест к разделу 1.

Модуль 2. Киберкультура. (12 часов)

Теория. Киберкультура. От книги к гипертексту. Киберкнига. Киберискусство. Социальная инженерия. Классификация угроз социальной инженерии.

Практика. Практикум к разделу 2. Практическая работа от компа-ний мобильной связи Билайн, МТС и Мегафон (по выбору учащихся).

Тест к разделу 2.

Модуль 3. Киберугрозы (11 часов)

Теория. Кибервойны. Киберпреступность. Примеры киберпресту- плений. Уязвимости кибербезопасности. Угрозы информаци-онной безопасности. Запрещенные и нежелательные сайты. Новые профессии в киберобществе.

Практика. Практикум к разделу 3 Практическая работа на основе он- лайн-курса Академии Яндекса «Безопасность в Интернете» (продолжение), по темам:

Защита от вредоносных программ.
Безопасность аккаунтов. Логины и пароли от электрон-ной почты, социальных сетей и других сервисов.
Тест к разделу 3.

Содержание курса (10-11 класс)
(36 часов)

Модуль 1. Правовые основы информационной безопасности (5 ч.)

Теория. Основные документы в области информационной безопасности Российской Федерации. Субъективная и объективная стороны юридической ответственности.

Практика Информация как объект правовых отношений. Функции, принципы и виды юридической ответственности. Итоговое занятие. Подготовка презентации по теме в группах учащихся.

Модуль 2. Законодательство Российской Федерации о гражданско-правовой ответственности в сфере инфобезопасности (8 ч.)

Теория. Законодательство Российской Федерации о гражданско-правовой ответственности.

Практика Гражданско-правовая ответственность несовер-шеннолетних за проступки в области информационной безопасности (защиты информации). Итоговое занятие.Тест к модулю 2

Модуль 3. Законодательство Российской Федерации об административной ответственности в сфере инфобезопасности (12 часов)

Теория. Понятие административной ответственности. Административная ответственность несовершеннолетних граждан за проступки в области информационной безопасности (защиты информации).

Практика Ответственность за проступок в области нарушения авторских прав на лицензионное программное обеспечение. Итоговое занятие.Тест к модулю 3.

Модуль 4. Законода-тельство Российской Федерации об уголовной ответственности в сфере инфобезопасности (11 часов)

Теория. Понятие уголовной ответственности.

Практика Уголовная ответственность несовершеннолетних за преступления в области информационной безопасности (защиты информации). Итоговое занятие. Подготовка и защита проекта по теме.

4.Контрольно-оценочные средства

В процессе реализации образовательной программы проводятся диагностики с целью:

- мониторинга освоения обучающимися разделов дополнительной образовательной программы;
- мониторинга достижения обучающимися планируемых результатов (входящий, промежуточный, итоговый).

Используются методики, разработанные на основе классических методов и приемов и на основе педагогического опыта коллег.

Результаты освоения обучающимися программы обучения отслеживаются следующими видами контроля:

входящий (тестирование знаний, умений, навыков);

текущий (самостоятельная работа, выставки в конце каждого раздела, тестирование знаний, умений, навыков);

Контроль за знаниями и умениями, полученными обучающимися на занятиях, осуществляется в виде:

проверки знаний на каждом занятии (в форме групповой или индивидуальной беседы);
контрольного теоретического теста или практических проверочных работ в конце изучения темы;

в конце всего курса - защита творческой работы.

Для отслеживания результатов обучения применяется система проверочных работ по каждой теме.

Проверочная работа может быть организована:

в виде самостоятельной практической работы, в которой проверяется знания и навыки работы обучающихся по определенной теме программы;

в виде теста по теоретическому материалу, если изученная тема носит преимущественно теоретический характер (например, тема «Устройство персонального компьютера», «А вы это знали?»).

Оценивание выполненной практической работы производится по пятибалльной системе, так как она наиболее привычна для восприятия обучающимися:

Отлично (5) - работа выполнена полностью, ответы правильные, навыки работы с программой устойчивые, есть своя «изюминка».

Хорошо (4) - работа выполнена полностью, но есть недочеты, умения работы с программой приобретены, но еще не сформировались как навыки.

Удовлетворительно (3) - работа выполнена не полностью, есть существенные недочеты, с программой ребенок знаком, но не умеет ею пользоваться без подсказки педагога.

Выполнение теста оценивается также по пятибалльной шкале, соотнесение оценки с количеством правильных ответов зависит от количества вопросов теста:

свыше 80% правильных ответов - отлично (5);

от 50% до 80% правильных ответов - хорошо (4);

от 40% до 50% правильных ответов - удовлетворительно (3). **Результаты освоения программы определяются по трем уровням:**

продвинутый - материал освоен в полном объёме, с практической частью справляется полностью, проявляет творчество.

базовый - материал освоен в полном объёме, с практической частью справляется и с помощью педагога и самостоятельно, проявляет творчество.

стартовый - материал освоен не в полном объёме, с практической частью справляется с помощью педагога, творчество не проявляет или проявляет частично.

Пояснение: если обучающийся освоил программу только на стартовом уровне (или он просто школьник 1-2 класса), то он может на следующий год продолжить обучение по данной программе, но уже на базовом уровне. Аналогично можно пройти обучение с базового на продвинутый уровень.

Итоговое занятие проводится в форме защиты творческой работы, подразумевающей выставление отметок за знания и умения. **Формы аттестации**

Формы контроля успешности обучающихся и подведения итогов реализации программы:

Результативность работы планируется отслеживать в течение учебного года на занятиях путем педагогического наблюдения (развитие каждого ребенка и группы в целом).

Текущий контроль предполагается проводить на каждом занятии - подведение итогов с перспективой на будущее, диалоги, игры на развитие логики, внимания, памяти.

Промежуточный контроль проводится после изучения каждой темы - обобщающее повторение (проведение тестов на знание теоретического материала и практические задания).

Итоговый контроль предполагает анализ усвоения образовательной программы обучающимися.

Периодичность проверки образовательных результатов и личностных качеств обучающихся:

сентябрь - входной контроль (опрос, педагогическое наблюдение, тест «Устройство компьютера») текущий контроль (наблюдение на каждом занятии, само- и взаимооценка)

декабрь - промежуточный контроль (практические задания)

апрель-май - итоговая диагностика (защита творческих проектов).

5.Условия реализации программы

Модули данной программы разработаны в соответствии с учетом возрастных особенностей и потребностей детей. Освоение модулей предполагает разделение на ***четыре возрастные группы***:

- **2-4 класс** (модули «Правила безопасной работы в сети Интернет с мобильным телефоном», «Правила безопасной работы в сети Интернет с планшетом или на компьютере», «Путешествуем в сети Интернет»», «Правила безопасной работы в социальной сети»)
- **5-6 класс** (модули «Что нужно знать? Пространство Интернета на планете Земля», Что нужно уметь? Правила пользоыателей сети Интернет»)
- **7-9 класс** (модули «Киберпростанство», «Киберкультура», «Киберугрозы»)
- **10-11 класс** (модули «Правовые основы информационной безопасности», «Законодательство РФ о гражданско-правовой ответственности в сфере инфобезопасности», «Законодательство РФ об административной ответственоети в сфере инфобезопасности», 2законодательство РФ об уголовной ответственоети в сфере инфобезопасности»)

Занятия в каждой группе проходят под руководством педагога дополнительного образования по направлению «Информатика» ЦОЦиГП «Точка роста» 1 раз в неделю по 1 ч.

Уроки информационной безопасности несут практическую направленность.

Познавательная часть урока основана на постановке учителем проблемы в качестве темы урока, ее рекомендуется проводить в форме беседы-дискуссии, опираясь на видео-материалы и факты по теме. Рекомендуется на каждом уроке в рамках изучаемой темы:

- рассказать школьникам о возможных негативных последствиях, которые могут наступить при работе в сети Интернет;
- мотивировать школьников использовать ресурсы сети Интернет для определенных целей;
- выстроить беседы в максимально доверительном тоне. Доверие между ребенком и взрослым — залог успеха в таком важном деле;

- использовать компьютерный класс, где установлена аппаратная защита — постоянно обновляемый анти-вирус, программа защиты (контент-фильтр) для сортировки и отсеивания информации негативного характера;
- активно вовлекать детей в обсуждение проблемы по теме.

Практическая часть урока основана на выполнении заданий по работе с информацией по теме, в том числе практических работ от ведущих ИТ-компаний, специально разработанных для детей и представленных в открытом доступе. Все уроки по темам курса снабжены тестами для промежуточного контроля, которые удобно проводить в форме мини-викторин.

Учебно-методическое обеспечение программы

Для достижения планируемых результатов предусмотрены учебно-методические комплекты по информационной безопасности для 2-4, 5-6, 7-9 и 10-11 классов [2, 3, 4, 5], снабженных открытыми электронными материалами на сайте издательства БИНОМ [6].

В состав интернет-ресурсов для проведения занятий по информационной безопасности включены открытые курсы и электронные материалы, видеоролики от ведущих ИТ-компаний и операторов мобильных сетей [7, 8, 9, 10, 11].

Курс представлен в учебном пособии «Информационная безопасность. Правила безопасного Интернета. 2-4 классы». К учебному пособию на сайте издательства размещено бесплатное электронное приложение. Оно включает ресурсы для выполнения практических заданий к урокам из пособия, а также открытые познавательные ресурсы для 2-4 классов.

http://lbz.ru/metodist/authors/ib/2-4.php

Перечень электронных приложений к модулям (Приложение 2)

Материально - техническое обеспечение программы

Обновленная материально-техническая база ЦОЦиГП «Точка роста» удовлетворяет все требования к обеспечению курса:

- ПК - 10 шт.
- Медиапроектор, интерактивный комплекс - 1 шт.
- Принтер - 1 шт.
- Сканер - 1 шт.
- Операционная система Windows 10
- Стандартные программы Open Office
- Выход в сеть Интернет
- Аудио колонки

6.Список литературы для педагогов

1.Роскомнадзор, официальный сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, URL: http://rkn.gov.ru/

2. Цветкова М. С., Якушина Е. В. Информационная безопас-ность. Правила безопасного Интернета. 2-4 классы : учеб-ное пособие.— М.: БИНОМ. Лаборатория знаний, 2020. — 112 с.

3. Цветкова М. С., Якушина Е. В. Информационная безопас-ность. Безопасное поведение в сети Интернет. 5-6 классы : учебное пособие. — М.: БИНОМ. Лаборатория знаний, 2020. — 96 с.

4. Цветкова М. С., Хлобыстова И. Ю. Информационная безо-пасность. Кибербезопасность. 7-9 классы : учебное посо-бие. — М.: БИНОМ. Лаборатория знаний, 2020. — 64 с.

5. Цветкова М. С., Голубчиков С. В., Новиков В. К., Семибра- тов А. М., Якушина Е. В. Информационная безопасность: Правовые основы информационной безопасности. 10-11 классы : учебное пособие. — М.: БИНОМ. Лаборатория зна-ний, 2020. — 112 с.

6. Сайт электронного приложения к пособиям по инфор-мационной безопасности, URL: http://lbz.ru/metodist/ authors/ib/

7. «Безопасный Билайн», компания Билайн, URL: http:// moskva.beeline.ru/customers/help/safe-beeline/

8. «Безопасность», компания МТС, URL: http://www.safety. mts.ru/ru/

9. «Безопасное общение», компания Мегафон, URL: http:// moscow.megafon.ru/bezopasnoe_obschenie/

10. «Памятка по безопасному общению», компания Мегафон, URL: http://moscow.megafon.ru/download/~msk/~moscow/ stopfraud/brochure.pdf

11. Открытый онлайн-курс «Безопасность в Интернете», «Академия Яндекс», компания Яндекс, URL: https:// academy.yandex.ru/events/online-courses/internet_security/

Приложение 1

Мониторинг образовательной деятельности обучающихся

Карта «Оценка уровня компетентности обучающихся»

Карта «Оценка уровня мотивации образовательной деятельности обучающихся»

Педагог дополнительного
образования _____

№	ФИ обучающегося	**МЕТАПРЕДМЕТНЫЕ РЕЗУЛЬТАТЫ**																
		КОММУНИКАТИВНЫЕ УУД				**РЕГУЛЯТИВНЫЕ УУД**				**ПОЗНАВАТЕЛЬНЫЕ УУД**				**ЛИЧНОСТНЫЕ УУД**				
		1	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**5**
1																		
2																		
3																		
4																		
5																		
6																		
7																		
8																		
9																		
10																		
11																		
12																		
13																		
14																		
15																		
№	ФИ обучающегося	**ПРЕДМЕТНЫЕ РЕЗУЛЬТАТЫ**																
		1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**						
1																		
2																		
3																		
4																		
5																		
6																		
7																		
8																		
9																		
10																		
11																		
12																		
13																		
14																		
15																		

Приложение 2

Перечень электронных прилржений к модулям курса

№	**Курс/модуль**	**Электронное приложение**
	Курс 2-4 класс	

1	**Модуль 1. Правила безопасной работы в сети Интернет с мобильным телефоном**	http://lbz .ru/metodist/authors/ib/2-4.php
		видеоурок СПАС Экстрим «Мобильные мошенники».
2	**Модуль 2. Правила безопасной работы в сети Интернет с планшетом или на компьютере**	http://lbz .ru/metodist/authors/ib/2-4.php
		Пособие компании МТС для младших школьников с сайта «Дети в Интернете». Распечатай, прочитай тексты и раскрась картинки, чтобы получить собственное настольное пособие. (http://www.safety.mts.ru/ru/deti_v_inete/for_ children/rules/)
		видеоурок СПАС Экстрим «Безопасный Интернет».
3	**Модуль 3. Путешествуем в сети Интернет**	http://lbz .ru/metodist/authors/ib/2-4.php
		Сайт детской безопасности Министерства чрезвычайных ситуаций.
		Электронное учебное пособие «Учимся беречь энергию» «Началка.инфо».
		Сайт Lingualeo. Покори язык. Lingualeo — это увлекательный, эффективный и бес-платный сервис для изучения английского языка. Сайт Учи.ру. Учащиеся из всех регионов России изучают школьные предметы в интерактивной форме. *йт «Российская электронная школа».* Сайт с материалами окружающем мире. Сайт Московского планетария. Сайт коллекций Московского планетария поможет познакомиться с миром космоса. Московский зоопарк. Видео. Живое видео из вольеров зоопарка поможет проводить наблюдения за жизнью животных в зоопарке, что поможет в изучении окружающего мира. *Сайт «Культура России».* Коллекции творчества народов России, информация о театрах и музеях нашей страны, культурное наследие — все это поможет развивать свои знания и поможет в уроках по искусству и технологии *Национальная электронная детская библиотека.* Зарегистрируйся в библиотеке, пользуйся ресурсами.
4	**Модуль 4. Правила безопасной работы в социальной сети**	http: //lbz .ru/metodist/authors/ib/2-4.php
		Курс 5-6 класс
1.	**Модуль Что нужно знать? Пространство Интернета на планете Земля**	http://lbz.ru/metodist/authors/ib/5-6.php
		Сайт «Защита детей. Лаборатория Касперского». Мультфильм «Приключения робота Каспера — Лайкомания»
		Сайт «Безопасный Интернет для детей»: http: //i-deti.org/video/ Видеоролик «Угрозы Интернета для детей» Видеоролик «Мировой опыт защиты детей в Интернете»
		2. Сайт телеканала «Карусель»: https://www.karusel-tv.ru/ Видеоролик «Почемучка. Где находится Интернет?». https://www.karusel-tv.ru/ «Почемучка. Что такое веб-браузер»?
		Детская социальная сеть «Лунтик»: www.luntik.ru, представляющая российские и зарубежные мультфильмы для детей
		Сайт телеканала «Карусель»: https://www.karusel-tv. ги/, видеоурок «Почемучка. Вирусы» 1. Сайт «Защита детей. Лаборатория Касперского». 1. Мультфильм «Приключения робота Каспера — Кибербуллинг»: https://kids.kaspersky.ru/ entertainment/multfilmy/priklyucheniya-robota-kaspera-kiberbulling/; Мультфильм «Приключения робота Каспера — Фишинг»: https://kids.kaspersky.ru/entertainment/

		multfilmy/priklyucheniya-robota-kaspera-fishing/
		Сайт «Защита детей. Лаборатория Касперского»: Фиксики: Фикси-советы: Осторожней в Интернете! — Конфиденциальность: https://kids.kaspersky.ru/ entertainment/ficksics/fiksi-sovety-ostorozhnej-v- internete-konf identsialnost/ Мультфильм «Приключения робота Каспера — Общение в игре»: https://kids.kaspersky.ru/ entertainment/multf ilmy/priklyucheniya-robota- kaspera-privatnost-akkauntov-2/
		Сайт «Защита детей. Лаборатория Касперского». Мультфильм «Приключения робота Каспера — Овершеринг. Вред репутации»: https://kids.kaspersky. ru/entertainment/multfilmy/priklyucheniya-robota-kaspera-overshering-vred-reputatsii/
		Сайт «Лига безопасного Интернета» Практикум «Азбука информационной безопасности» (Лаборатория Касперского): http://ligainternet.ru/ upload/docs/docs-f or-dowloud/Azbuka_ informatsionnoy_bezopasnosti.pdf
2	**Модуль 2. Что нужно уметь? Правила для пользователей сети Интернет**	Сайт «Защита детей. Лаборатория Касперского»: Мультфильм «Приключения робота Каспера — Друг Вовка»: https://kids.kaspersky.ru/entertainment/ multfilmy/priklyucheniya-robota-kaspera-drug-vovka/ Мультфильм «Приключения робота Каспера — Приватность аккаунтов»: https://kids.kaspersky. ru/entertainment/multfilmy/priklyucheniya-robota-kaspera-privatnost-akkauntov/
		Сайт «Защита детей. Лаборатория Касперского». Мультфильм «Приключения робота Каспера — Сообщения со взломанных аккаунтов»: https://kids. kaspersky.ru/entertainment/multfilmy/priklyucheniya-robota-kaspera-soobshheniya-so-zlomannyh-akkauntov/
		Сайт «Защита детей. Лаборатория Касперского». Фиксики: Фикси-советы: Осторожней в Интернете! — Тролли: https://kids.kaspersky.ru/entertainment/ f icksics/f iksisovetyostorozhnej - v-internete-trolli/
		Сайт «Защита детей. Лаборатория Касперского». Фиксики: Фиксики — Вирус: https://kids.kaspersky. ru/entertainment/f icksics/f iksiki-virus-f ixiki /
		Сайт «Защита детей. Лаборатория Касперского». Мультфильм «Приключения робота Каспера — Мошенничество в Интернете»: https://kids.kaspersky.ru/entertainment/multfilmy/ priklyucheniya-robota-kaspera-moshennichestvo-v-internete/
		Сайт «Защита детей. Лаборатория Касперского»: Мультфильм «Приключения робота Каспера — Опасности на надежных сайтах»: https://kids. kaspersky.ru/entertainment/opasnosti_na-saitah/ Фиксики: Фикси-советы: Осторожней в Интернете! — Встроенные покупки: https:// kids .kaspersky. ru/entertainment/f icksics/f iksi- sovetyostorozhne j-v-internete-vstroennye-pokupki/
		Сайт «Защита детей. Лаборатория Касперского». Фиксики: Фикси-советы: Осторожней в Интернете! — Профили: https://kids.kaspersky.ru/entertainment/ ficksics/fiksi-sovetyostorozhnej-v-internete-profili/
		Система помощи в социальной сети ВКонтакте: https: //vk .com/support Система помощи в социальной сети Facebook: https:// www. f

		acebook .com/help/ Система помощи в социальной сети Одноклассники: https://www.ok.ru/help Ознакомьтесь с видеоматериалами. Составьте памятку поведения в социальных сетях на тему информационной безопасности. Сайт телеканала «Карусель»: https://www.karusel- tv.ru/ Видеоурок «Почемучка. Как вести себя в социальных сетях?»
		Сайт «Безопасный Интернет для детей»: http://i-deti. org/ Как обнаружить ложь и остаться правдивым в Интернете: http://i-deti.org/video/ • Защита персональных данных. Детская безопасность в Интернете: http://i-deti.org/video/
		Сайт «Пространство безопасности. Школа первой помощи». Раздел «Телефоны первой помощи»: http://allsafety. ru/f irst_aid/telef on. htm
		Российская государственная детская библиотека: https://rgdb.ru/ Раздел «Национальная электронная детская библио-тека»: http://arch.rgdb.ru/xmlui/
		http://audiohrestomatiya.ru/ «Аудиохрестоматия» — это медиапортал, на котором собраны произведения мировой литературы в испол-нении известных артистов, а также биографии писате-лей.
		Сайт Всероссийского общества слепых: http://www. vos.org.ru/ Для поддержки людей с ограниченными возможностями по зрению специально создан социально-информационный проект Nvda.ru. Бесплатная программа экранного доступа Nvda: https: / / nvda. ru /
Курс 7-9 класс		
1	**Модули 1-3**	**http://lbz.ru/metodist/authors/ib/7-9.php**
Курс 10-11 класс		
1	**Модули 1-4**	**http://lbz.ru/metodist/authors/ib/10-11.php**