МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«СРЕДНЯЯ ШКОЛА № 8 С УГЛУБЛЕННЫМ ИЗУЧЕНИЕМ ИНОСТРАННЫХ ЯЗЫКОВ» ГОРОДА СМОЛЕНСКА

РАССМОТРЕНО Заведующий кафедрой точных наук _____/ / Протокол № ____от «____» августа 2020г	СОГЛАСОВАНО Председатель НМС _____/ / ____ августа 2020 г.	УТВЕРЖДЕНО Заместитель директора _____/ ___ августа 2020 г.

РАБОЧАЯ ПРОГРАММА

ЭЛЕКТИВНОГО КУРСА

Основы информационной безопасности

предметная область – математика и информатика

11 класс

Составитель
Чердакова М.Н.,
учитель информатики
(высшая квалификационная категория)

2020-2021 учебный год

I. КОМПЛЕКС ОСНОВНЫХ ХАРАКТЕРИСТИК ПРОГРАММЫ

Пояснительная записка

Данная программа элективного курса под названием «Основы информационной безопасности» отнесена к программам **технической направленности**. Ее цель и задачи направлены на систематизацию знаний и навыков по безопасному поведению учащихся при работе с информацией.

Новый этап развития человечества с построением глобального цифрового пространства требует знания информационно-цифровой грамотности от каждого члена общества. Для развития информационного общества важнейшим направлением является цифровая грамотность. Программа ЮНЕСКО «Информация для всех» (IFAP) определяет цифровую грамотность как важнейший жизненныйнавык.

Цифровая грамотность – это умение пользоваться цифровыми устройствами, понимание современных технологий и их безопасное и эффективное использование, навыки корректной работы с информацией и даже соблюдение определенных мер безопасности в цифровой среде. Это понятие охватывает такие направления, как безопасность в интернете, цифровая тень, кибербуллинг и цифровая этика. Например, какой информацией можно делиться в социальных сетях, а какой нельзя, как не стать жертвой мошенников, как предотвратить плагиат и многое другое.

Цифровая грамотность включает в себя: цифровое потребление; цифровые компетенции; цифровую безопасность. Цифровая безопасность – основы безопасности в Сети. Включает в себя: защиту персональных данных, надежный пароль, легальный контент, культуру поведения, репутацию, этику, хранение информации, создание резервных копий.

Деятельность в рамках занятий элективного курса «Основы информационной безопасности» направлена на расширение, углубление и систематизацию знаний по основам безопасной работы с информацией.

Диапазон предложенных тем позволяет охватить все сферы, в которых человек взаимодействует с информацией.

Актуальность программы заключается в том, что формирование у детей цифровой компетентности (а вместе с ней и цифровой безопасности), позволяющей им безопасно ориентироваться в информационной среде, является первостепенной задачей, которая стоит перед образовательной и воспитательной системами. Кроме этого, актуальность подкреплена Распоряжением Правительства РФ от 02.12.2015 года утвердить Концепцию информационной безопасности детей. В которой поставлены приоритетные для государства, семьи и школы задачи в обеспечении информационной безопасности детей:

«….развитие у детей навыков самостоятельного и ответственного потребления информационной продукции;

повышение уровня медиаграмотности детей;

развитие у детей чувства ответственности за свои действия в информационном пространстве.». Эти же задачи легли в основу данной рабочей программы.

Место программы в системе государственных программ. Рабочая программа элективного курса «Основы информационной безопасности» для 11 класса разработана на основе федерального государственного образовательного стандарта основного общего образования (ФГОС СОО); требований к результатам освоения основной образовательной программы (личностным, предметным, метапредметным); основных подходов к развитию и формированию универсальных учебных действий (УУД) для среднего общего образования, основной образовательной программы. Примерные рабочие программы данной тематики для среднего общего образования отсутствуют. Данная программа составлена, опираясь на примерную программу учебной дисциплины «Основы информационной безопасности», разработанную на основе федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем».

Особенность и новизна программы заключается в том, что в курсе рассматриваются вопросы влияния информации на формировании личности и на психическое и физическое здоровье человека. Сегодня каждый из нас вынужден перерабатывать такие объемы информации, которые еще 10 лет назад казались немыслимыми. Специалисты утверждают, что с начала двухтысячных количество информации на планете удваивается. Такая ситуация приводит к тому, что влияние информации на человека увеличивается многократно. Вне зависимости от нашего желания этот процесс происходит постоянно, и с каждым новым днем его сила и давление только возрастает.

Хорошо, если это воздействие оказывает положительное влияние на личность человека. Однако, чаще всего приходится сталкиваться с негативными последствиями информационного влияния. А если это так, то просто необходимо быть максимально осведомленными в вопросе противодействия такому влиянию.

Педагогическая целесообразность программы заключается в том, что именно в старшем школьном возрасте подросток имеет большой опыт в работе с информацией. Реализация **программы** принимает дискуссионный характер с опорой на личностные ситуации и переживания ребенка. Применяемые на занятиях методы обучения и содержательный компонент **программы** в полной мере отвечают возрастным особенностям старших школьников. Данная общеобразовательная общеразвивающая программа «Основы информационной безопасности» может быть использована в любом учреждении основного или дополнительного образования и адаптирована под кадровые и материальные ресурсы учреждения.

Адресат программы. Рабочая программа элективного курса «Основы информационной безопасности» разработана для учащихся 10-11 класса.

Объем и срок освоения программы. Программа рассчитана на 34 часа (1 час в неделю). Срок реализации рабочей программы – один учебный год. Периодичность проведения занятий: 1раз в неделю. Продолжительность одного занятия – 40 минут. Оптимальная наполняемость учебной группы – от 10 до 15человек.

Формы организации образовательного процесса

Содержание учебного материала, формы и методы работы отобраны с учетом потребностей и возрастных особенностей учащихся, не создают учебных перегрузок, так же учитываются индивидуально-типологические особенности личности (способности, интересы, склонности, особенности интеллектуальной деятельности, возраст обучаемых).

Форма проведения занятий планируется для всей группы. Формы организации деятельности учащихся на занятии: групповая, по подгруппам, индивидуальная.

Виды занятий по программе:

- беседы;
- проблемные лекции;
- практические занятия;
- пресс-конференция;
- семинар;
- тематическая дискуссия;
- диспут;
- групповая консультация.

Дляорганизацииучебногопроцессаиспользуютсятакие**методы**как:

- информационно-рецептивные,
- объяснительно-иллюстративные,
- репродуктивные,
- частично-поисковые.

Цель и задачи программы

Данный курс преследует следующую **цель**: систематизация знаний и навыков по безопасному поведению учащихся при работе с информацией.

Задачи курса:

- развитие у детей навыков самостоятельного и ответственного потребления информационной продукции;

– повышение уровня медиаграмотности детей;

– развитие у детей чувства ответственности за свои действия в информационном пространстве;

– расширить знанияи умения, в рамках тематики программы, полученные на уроках ОБЖ и информатики;

– освоение учащимися знаний, относящихся к основам обеспечения информационной безопасности, и их систематизация;

– изучение учащимися мер законодательного, административного, процедурного и программно-технического уровней при работе на компьютерах и в компьютерных сетях;

– приобретение учащимися навыков самостоятельной работы с учебной, научно-популярной литературой и материалами сети Интернет;

– воспитание у учащихся нравственных качеств, негативного отношения к нарушителям информационной безопасности;

– воспитание у учащихся установки на позитивную социальную деятельность в информационном обществе, недопустимость действий, нарушающих правовые и этические нормы работы с информацией.

Планируемые результаты

Планируемые результаты по программе соотнесены с задачами и содержанием программы. Обучающиеся к концу обучения должны иметь следующие результаты:

Личностными результатами обучающихся являются:

– готовность к самоидентификации в окружающем мире на основе критического анализа информации, отражающей различные точки зрения на смысл и ценности жизни;

– владение навыками соотношения получаемой информации с принятыми в обществе моделями, например, морально-этическими нормами, критическая оценка информации в СМИ;

– умение создавать и поддерживать индивидуальную информационную среду, обеспечивать защиту значимой информации и личную информационную безопасность, развитие чувства личной ответственности за качество окружающей информационной среды;

– приобретение опыта использования информационных ресурсов общества и электронных средств связи в учебной и практической деятельности; освоение типичных ситуаций по настройке и управлению персональных средств ИКТ, включая цифровую бытовую технику;

– умение осуществлять совместную информационную деятельность, в частности при выполнении учебных проектов;

– повышение своего образовательного уровня и уровня готовности к продолжению обучения с использованием ИКТ.

– формирование ответственного отношения к учению, готовности и способности, обучающихся к саморазвитию и самообразованию на основе мотивации к обучению и познанию;

– формирование целостного мировоззрения, соответствующего современному уровню развития науки и общественной практики;

– развитие осознанного и ответственного отношения к собственным поступкам; формирование коммуникативной компетентности в процессе образовательной, учебно-исследовательской, творческой и других видов деятельности.

Метапредметными результатами обучающихся являются:

– умение самостоятельно определять цели своего обучения, ставить и формулировать для себя новые задачи в учёбе и познавательной деятельности, развивать мотивы и интересы своей познавательной деятельности;

– владение основами самоконтроля, самооценки, принятия решений и осуществления осознанного выбора в учебной и познавательной деятельности;

– умение определять понятия, создавать обобщения, устанавливать аналогии, классифицировать, самостоятельно выбирать основания и критерии для классификации, устанавливать причинно-следственные связи, строить логическое рассуждение, умозаключение (индуктивное, дедуктивное и по аналогии) и делать выводы;

– умение создавать, применять и преобразовывать знаки и символы, модели и схемы для решения учебных и познавательных задач;

– смысловое чтение; умение осознанно использовать речевые средства в соответствии с задачей коммуникации;

– формирование и развитие компетентности в области использования информационно-коммуникационных технологий (далее ИКТ - компетенции).

– владение навыками постановки задачи на основе известной и усвоенной информации и того, что ещё неизвестно;

– планирование деятельности: определение последовательности промежуточных целей с учётом конечного результата, составление плана и последовательности действий;

– прогнозирование результата деятельности и его характеристики;

– контроль в форме сличения результата действия с заданным эталоном;

– коррекция деятельности: внесение необходимых дополнений и корректив в план действий;

– умение выбирать источники информации, необходимые для решения задачи (средства массовой информации, электронные базы данных, информационно-телекоммуникационные системы, Интернет, словари, справочники, энциклопедии и др.);

– умение выбирать средства ИКТ для решения задач из разных сфер человеческой деятельности;

– выбор языка представления информации в модели в зависимости от поставленной задачи.

Предметными результатами обучающихся являются:

– понимание основных проблем защиты информации;

– следование нормам жизни и труда в условиях информационной цивилизации;

– приобретение опыта выявления информационных технологий, разработанных со скрытыми целями;

– соблюдение норм этикета, российских и международных законов при передаче информации по телекоммуникационным каналам;

– расширение представления о правовых и морально-этических нормах в информационной сфере, законодательстве Российской федерации в области защиты информации и авторского права;

– формирование чувства ответственности за производство и распространение информации;

– понимание роли информационных процессов как фундаментальной реальности окружающего мира и определяющего компонента современной информационной цивилизации;

– определение средств информационных технологий, реализующих основные информационные процессы;

– понимание принципов действия различных средств информатизации, их возможностей и технических и экономических ограничений;

– выбор средств информационных технологий для решения поставленной задачи;

– приобретение опыта создания и преобразования информации различного вида, в том числе с помощью компьютера;

– приобретение опыта создания эстетически значимых объектов с помощью возможностей средств информационных технологий (графических, цветовых, звуковых, анимационных);

– понимание особенностей работы со средствами информатизации, их влияния на здоровье человека, владение профилактическими мерами при работе с этими средствами;

– приобретение навыков защиты информации;

– соблюдение требований безопасности и гигиены в работе с компьютером и другими средствами информационных технологий.

В результате прохождения программного материала

Обучающиеся научатся:

– объяснять необходимость изучения проблемы информационной безопасности;

– применять методы профилактики и защиты информационных ресурсов от вредоносного программного обеспечения;

– соблюдать права интеллектуальной собственности на информацию;

– применять методы ограничения, контроля, разграничения доступа, идентификации и аутентификации;

– производить простейшие криптографические преобразования информации;

– планировать организационные мероприятия, проводимые при защите информации;

– применять методы защиты информации в компьютерных сетях;

– различать основные виды информационно-психологических воздействий в виртуальной реальности;

– соблюдать требования информационной безопасности, этики и права.

Обучающие получат возможность научиться:

– искать и обрабатывать информацию из различных источников, приводить собственные примеры явлений и тенденций, связанных с безопасностью информационного общества;

– интерпретировать изучаемые явления и процессы, давать им сущностные характеристики, высказывать критическую точку зрения и свои суждения по проблемным вопросам;

– сравнивать, анализировать и систематизировать имеющийся учебный материал;

– участвовать в групповой работе и дискуссиях, решении задач в игровых ситуациях и проектной деятельности.

Содержание программы

№	Название раздела	Название темы	Количество часов	Формы аттестации\ контроля
1	**Информация и право (7 часов)**	Информация. Источники информации.	1	Текущий контроль
		Информация как объект преступных посягательств.	1	Текущий контроль
		Информация как средство совершения преступлений.	1	Текущий контроль
		Классификация мер защиты информации	1	Текущий контроль
		Криптография и защита информации.	1	Текущий контроль
		Защита интеллектуальной собственности. Авторское право и тиражирование	1	Текущий контроль
		Государственная тайна как особый вид защищаемой информации	1	Текущий контроль
2	**Информация и личность (5 часов)**	Виды информационных воздействий	1	Текущий контроль
		Угрозы информационной безопасности.	1	Текущий контроль
		Роль информации в обеспечении личной безопасности.	1	Текущий контроль
		Защита персональной информации	1	Текущий контроль
		Информация и права потребителя	1	Текущий контроль
3	**Информация и здоровье (5 часов)**	Влияние информации на здоровье человека.	1	Текущий контроль
		Оценка информационных влияний	1	Текущий контроль

		Виртуальная реальность	1	Текущий контроль
		Дезинформация. Реклама.	1	Текущий контроль
		Методы и средства защиты человека от негативного воздействия информации	1	Текущий контроль
4	**Информация и общество (5 часов)**	Роль информации в социальных отношениях	1	Текущий контроль
		Негативные проявления массовой культуры	1	Текущий контроль
		Информационная безопасность и СМИ.	1	Текущий контроль
		Информационная война	1	Текущий контроль
		Информационный терроризм	1	Текущий контроль
5	**Информация и компьютер (4 часа)**	Условия использования программного обеспечения	1	Текущий контроль
		Виды угроз для цифровой информации	1	Текущий контроль
		Вредоносное программное обеспечение	1	Текущий контроль
		Антивирусное ПО	1	Текущий контроль
6	**Информация и Интернет (7 часов)**	Причины уязвимости сети Интернет.	1	Текущий контроль
		Виды и особенности сетевых информационных угроз (кибербуллинг, мошенничество, интернет-преступления)	3	Текущий контроль
		Формы контроля над информационными потоками	1	Текущий контроль
		Программные средства родительского контроля	1	Текущий контроль
		Обеспечение информационной безопасности обучающихся. Системы контентной фильтрации.	1	Текущий контроль
Промежуточная аттестация			1	Промежу-точный контроль
		Итого:	***34***	

Содержаниеучебного(тематического)плана

№	Название темы	Содержание темы
Информация и право(7 часов)		
1	Инструктаж по ТБ и ОТ Информация. Источники информации.	*Теория*:целиизадачи,структуракурса.Техникабезопасности и охрана труда *Практика:* Зачетпо ТБ
2	Информация как объект преступных посягательств.	*Теория*:Свобода доступа к информации и свобода ее распространения
3	Информация как средство совершения преступлений.	*Теория*:Правовое регулирование в информационной сфере. *Практика: Работа с УК РФ*
4	Классификация мер защиты информации	*Теория*: Меры защиты информации *Практика:Работа с ФЗ № 149*

5	Криптография и защита информации.	*Теория*:Криптография и защита информации. ЭЦП и сертификаты *Практика: Работа с шифрами*
6	Защита интеллектуальной собственности. Авторское право и тиражирование	*Теория*:Защита интеллектуальной собственности. Авторское право и тиражирование *Практика: Знакомство с законом Об информатизации и документами на патент*
7	Государственная тайна как особый вид защищаемой информации	*Теория*:Информационная безопасность как составляющая национальной безопасности. *Практика: Знакомство с законом О государственной тайне*
Информация и личность (5 часов)		
8	Виды информационных воздействий	*Теория*:Виды информационных воздействий. Информационная безопасность *Практика: Анкета Определение уровня интернет-зависимости*
9	Угрозы информационной безопасности.	*Теория*:Угрозы информационной безопасности.
10	Роль информации в обеспечении личной безопасности.	*Теория*:Роль информации в обеспечении личной безопасности. *Практика: упражнение Мой профиль*
11	Защита персональной информации	*Теория*: Понятие персональных данных. Защита персональной информации. *Практика: упражнение Великий идентификатор*
12	Информация и права потребителя	*Теория*:Информация и права потребителя. *Практика: знакомство с законом О защите прав потребителей*
Информация и здоровье (5 часов)		
13	Влияние информации на здоровье человека.	*Теория*:Влияние информации на психическое и физическое здоровье человека *Практика: анкета Влияние компьютера на здоровье школьника*
14	Оценка информационных влияний	*Теория*:Оценка информационных влияний (мотив, цель, средства, реальные результаты). *Практика:опрос Как информация влияет на общество*
15	Виртуальная реальность	*Теория*: Технические средства виртуальной реальности
16	Дезинформация. Реклама.	*Теория*: Дезинформация. Реклама
17	Методы и средства защиты человека от негативного воздействия информации	*Теория*:Методы и средства защиты человека от негативного воздействия информации
Информация и общество (5 часов)		
18	Роль информации в социальных отношениях	*Теория*:Роль информации в социальных отношениях *Практика: Признаки цифровой диктатуры и цифровой*

		демократии
19	Негативные проявления массовой культуры	*Теория*:Негативные проявления массовой культуры
20	Информационная безопасность и СМИ.	*Теория*:Информационная безопасность и СМИ
21	Информационная война	*Теория*:Информационная война. *Практика: Как сократить угрозы, исходящие от информационной войны*
22	Информационный терроризм	*Теория*:Информационный терроризм
Информация и компьютер (4 часа)		
23	Условия использования программного обеспечения	*Теория*:Виды программного обеспечения (лицензионное, условно бесплатное, свободно распространяемое) *Практика: Знакомство с УК РФ (ст.146)и КоАП (ст. 7.2)*
24	Виды угроз для цифровой информации	*Теория*:Программно-технические меры обеспечения информационной безопасности (параметры безопасности)
25	Вредоносное программное обеспечение	*Теория*:Программно-технические меры обеспечения информационной безопасности (управление доступом)
26	Антивирусное ПО	*Теория*:Программно-технические меры обеспечения информационной безопасности (антивирусные программы) *Практика: Проверка компьютера при помощи антивирусного ПО*
Информация и Интернет (7 часов)		
27	Причины уязвимости сети Интернет.	*Теория*:Виды и особенности сетевых информационных угроз
28	Виды и особенности сетевых информационных угроз (кибербуллинг)	*Теория*:Кибербуллинг *Практика:Тест Что вы знаете о кибербуллинге?*
29	Виды и особенности сетевых информационных угроз (мошенничество)	*Теория*:Интернет-мошенничество *Практика:Кейс Мошенничество в сети*
30	Виды и особенности сетевых информационных угроз (интернет-преступления)	*Теория*:Интернет-преступления *Практика: Кейс Интетнет-преступления*
31	Формы контроля над информационными потоками	*Теория*:Необходимость различных форм контроля над информационными потоками.
32	Программные средства родительского контроля	*Теория*:Программы родительского контроля *Практика: Установка и настройка программ родительского контроля*
33	Обеспечение информационной безопасности обучающихся. Системы контентной фильтрации.	*Теория*:Системы контентной фильтрации. *Практика: Настройка программы контентной фильтрации*
34	Промежуточная аттестация	Итоговоетестированиеобучающихся

II. КОМПЛЕКС ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИХ УСЛОВИЙ

КАЛЕНДАРНЫЙ УЧЕБНЫЙГРАФИК

реализации дополнительной общеразвивающей программы технической направленности

«Основы информационной безопасности»

на2020/2021 учебныйгод

№	Название темы	Кол-во часов	Дата	Место проведения	Форма контроля
Информация и право (7 часов)					
1	Инструктаж по ТБ и ОТ Информация. Источники информации.	1		МБОУ СШ №8	Текущий контроль
2	Информация как объект преступных посягательств.	1		МБОУ СШ №8	Текущий контроль
3	Информация как средство совершения преступлений.	1		МБОУ СШ №8	Текущий контроль
4	Классификация мер защиты информации	1		МБОУ СШ №8	Текущий контроль
5	Криптография и защита информации.	1		МБОУ СШ №8	Текущий контроль
6	Защита интеллектуальной собственности. Авторское право и тиражирование	1		МБОУ СШ №8	Текущий контроль
7	Государственная тайна как особый вид защищаемой информации	1		МБОУ СШ №8	Текущий контроль
Информация и личность (5 часов)					
8	Виды информационных воздействий	1		МБОУ СШ №8	Текущий контроль
9	Угрозы информационной безопасности.	1		МБОУ СШ №8	Текущий контроль
10	Роль информации в обеспечении личной безопасности.	1		МБОУ СШ №8	Текущий контроль
11	Защита персональной информации	1		МБОУ СШ №8	Текущий контроль
12	Информация и права потребителя	1		МБОУ СШ №8	Текущий контроль
Информация и здоровье (5 часов)					
13	Влияние информации на	1		МБОУ СШ	Текущий

	здоровье человека.			№8	контроль
14	Оценка информационных влияний	1		МБОУ СШ №8	Текущий контроль
15	Виртуальная реальность	1		МБОУ СШ №8	Текущий контроль
16	Дезинформация. Реклама.	1		МБОУ СШ №8	Текущий контроль
17	Методы и средства защиты человека от негативного воздействия информации	1		МБОУ СШ №8	Текущий контроль
Информация и общество (5 часов)					
18	Роль информации в социальных отношениях	1		МБОУ СШ №8	Текущий контроль
19	Негативные проявления массовой культуры	1		МБОУ СШ №8	Текущий контроль
20	Информационная безопасность и СМИ.	1		МБОУ СШ №8	Текущий контроль
21	Информационная война	1		МБОУ СШ №8	Текущий контроль
22	Информационный терроризм	1		МБОУ СШ №8	Текущий контроль
Информация и компьютер (4 часа)					
23	Условия использования программного обеспечения	1		МБОУ СШ №8	Текущий контроль
24	Виды угроз для цифровой информации	1		МБОУ СШ №8	Текущий контроль
25	Вредоносное программное обеспечение	1		МБОУ СШ №8	Текущий контроль
26	Антивирусное ПО	1		МБОУ СШ №8	Текущий контроль
Информация и Интернет (7 часов)					
27	Причины уязвимости сети Интернет.	1		МБОУ СШ №8	Текущий контроль
28	Виды и особенности сетевых информационных угроз (кибербуллинг)	1		МБОУ СШ №8	Текущий контроль
29	Виды и особенности сетевых информационных угроз (мошенничество)	1		МБОУ СШ №8	Текущий контроль

30	Виды и особенности сетевых информационных угроз (интернет-преступления)	1		МБОУ СШ №8	Текущий контроль
31	Формы контроля над информационными потоками	1		МБОУ СШ №8	Текущий контроль
32	Программные средства родительского контроля	1		МБОУ СШ №8	Текущий контроль
33	Обеспечение информационной безопасности обучающихся. Системы контентной фильтрации.	1		МБОУ СШ №8	Текущий контроль
34	Промежуточная аттестация	1		МБОУ СШ №8	Промежуточный контроль

Условия реализации программы

Для реализации программы «Основы информационной безопасности» в образовательном учреждении созданы все необходимые условия для занятий: класс со свободным пространством, где можно получать теоретические знания 20 участникам, оборудованный необходимыми техническими средствами (компьютером, интерактивным комплексом, принтером).

Формы аттестации и контроля

В отслеживание успешности овладения учащимися содержания программы используются следующие методы отслеживания результативности:

– *педагогическое наблюдение;*

– *педагогический анализ результатов* анкетирования, тестирования, взаимозачётов, опросов, выполнения учащимися диагностических заданий, участия учащихся в мероприятиях, активности учащихся на занятиях и т.п.;

– *мониторинг.*

Проведение мониторинга: входящий, текущий и промежуточный контроль.

Входящий контроль: проводится с целью выявления способностей обучающихся. Его результаты позволяют определить уровни развития первоначального практического навыка и разделить детей на уровни мастерства. Это деление обеспечивает личностно-ориентированный подход в процессе обучения учебного занятия.

Текущий контроль является одним из основных видов проверки знаний, умений и навыков обучающихся. Ведущая задача текущего контроля - регулярное управление учебной деятельностью детей и ее корректировка. Он позволяет получить непрерывную информацию о ходе и качестве усвоения учебного материала и на основе этого оперативно вносить изменения в учебный процесс. Другими важными задачами текущего контроля является

стимуляция регулярной, напряженной деятельности; определение уровня овладения умениями самостоятельной работы, создание условий для их формирования.

Результаты выполнения программы каждым ребенком отслеживаются и оцениваются с помощью промежуточной и итоговой аттестации.

Промежуточный контроль проводится по итогам прохождения 60% программы.Для проведения процедуры оценки качества образования по факультативному курсу «Основы информационной безопасности» в рамках мониторинга образовательных достижений обучающихся 11 классов проводится промежуточная аттестация в форме теста.

Программой предусмотренопроведениепедагогическогодиагностирования,позволяющегоотследитьличностныеиметапредметные результатыучащихся.

Мониторинг сформированности личностных результатов	
Наименование личностного результата	**Название диагностической методики**
Уровень социальной адаптированности Цель: выявление уровня социальной адаптированности, активности, автономности и нравственной воспитанности учащегося	**Методика** Рожкова М И
Сформированность ценностных ориентаций личности	**Методика** Ш. Шварца (ценностный опросник Ш. Шварца)
Уровень школьной мотивации Цель: выявить отношение к школе, учебному процессу, эмоциональное реагирование на учебную ситуацию	**Методика** Лускановой Н.Г. Анкета «Оценка уровня школьноймотивации»
Мониторинг сформированности метапредметных результатов	
Наименование метапредметного результата	**Название диагностической методики**
Познавательные учебные действия	**Карта мониторинга УУД** по БуйловойЛ.Н., КленовойН.В
Регулятивныеучебныедействия Цель: диагностика уровня развития саморегуляции, организации деятельности, отдельных свойств внимания, объем оперативной памяти, прогноз успешности в обучении.	Диагностика интеллектуальной лабильности в модификации С.Н. Костроминой)
Коммуникативные учебные действия	Диагностика осуществляется в процессе наблюдения за обучающимися во время выполнения ими **групповых** заданий. Данные заносятся в карту наблюдений за особенностями общения и учеников в процессе совместного выполнения проекта.

УЧЕБНО-МЕТОДИЧЕСКОЕ И МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Учебно-методический комплект

1. Бабаш А., Баранова Е., Ларин Д. Информационная безопасность. История защиты информации в России. -М.: КДУ, 2015
2. Баранова Е.К., Бабаш А.В. Информационная безопасность и защита. Учебное пособие. – М.: РИОР, Инфра-М, 2016.
3. Вангородский С.Н., Основы кибербезопасности: учебно-методическое пособие. 5-11 классы. – М.: Дрофа, 2019.
4. Мельников В.П., Клейменов С.А., Петраков А.М.. Информационная безопасность и защита информации. – М.: Академия, 2016.
5. Нестеров С.А. Основы информационной безопасности – М.: Лань, 2016
6. Попов В.Б. Основы информационных и телекоммуникационных технологий. Основы информационной безопасности: Учебное пособие. - М.: Финансы и статистика, 2015.
7. Солдатова Г.У, Приезжева А.А., Олькина О.И., Шляпников В.И. Практическая психология безопасности: управление персональными данными в Интернете: учебно-методическое пособие для работников системы общего образования. - М.: Генезис, 2017.
8. Цветкова М.С., Новиков В.К., Голубчиков С.В. Правовые основы информационной безопасности. 10-11 классы. – М.: Бином. Лаборатория знаний, 2020.

Интернет-ресурсы

1. https://цифроваяграмотность.рф/
2. https://cryptoworld.su/
3. http://www.consultant.ru/
4. http://cgon.rospotrebnadzor.ru/
5. https://support.microsoft.com
6. https://www.kaspersky.ru/
7. https://www.avast.ru/
8. https://kids.kaspersky.ru/
9. https://растимдетей.рф/
10. https://kids.usafe.ru/
11. https://childhelpline.ru/

Технические средства обучения

1. Ноутбуки
2. Выход в сеть Интернет
3. Интерактивный комплекс

Программные средства

Антивирусное ПО

Приложение

МАТЕРИАЛЫ

для проведения промежуточной аттестации

по элективному курсу

«Основы информационной безопасности»

в 11 классах

Спецификация
контрольных измерительных материалов для проведения
промежуточной аттестации по факультативному курсу в 11 классах

Назначение КИМ

Итоговая работа предназначена для проведения процедуры оценки качества образования по элективному курсу «Основы информационной безопасности» в рамках мониторинга образовательных достижений обучающихся 11 классов. Проводится в соответствии с Федеральным законом от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации», Федеральным государственным образовательным стандартом.

Характеристика структуры и содержания работы

Форма проведения работы – ***Тест***.

Работа состоит из 10 вопросов на выбор правильного ответа из четырех предложенных. На проведение работы отводится 20 минут.

Распределение заданий КИМ по содержательным разделам курса, уровню сложности и видам проверяемых умений и способам действий.

Таблица 1

Блок содержания	Число заданий в работе
Информация и право	2
Информация и личность	2
Информация и здоровье	1
Информация и общество	2
Информация и компьютер	2
Информация и интернет	1
Итого	**10**

Система оценивания отдельных заданий и всей работы в целом

За верное выполнение заданий обучающийся получает 1 балл. За неверный ответ или его отсутствие - 0 баллов. Максимальное количество баллов, которое может набрать обучающийся верно выполнивший задания, – 10 баллов.

Шкала оценивания работы

«освоил» - 6-10 баллов

«не освоил» - менее 6 баллов

Промежуточная аттестация по курсу «Основы информационной безопасности», 11 класс

1. Что не относится к списку охраняемых результатов интеллектуальной деятельности?
1) топографические карты и планы
2) аранжировки и переводы
3) выведенная порода кошек
4) собственноручно приготовленный торт

2. Каких мер защиты информации из перечисленных не бывает?
1) Законодательные меры
2) Морально-этические меры
3) Интеллектуальные меры
4) Физические меры

3. Что из перечисленного относится к преднамеренным угрозам?
1) атака злоумышленников
2) разглашение конфиденциальной информации
3) установка ПО, которые могут стать причиной потери информации
4) проделки конкурирующих организаций

4. Какие угрозы ИБ можно отнести к искусственным?
1) удар молнии
2) потеря информации
3) наводнение
4) пожар

5. Что из перечисленного не относится к видам персональных данных?
1) получаемое образование
2) заработная плата
3) принадлежность к какой-либо неформальной группе
4) установленные на смартфоне приложения

6. Как часто нужно менять пароли?
1) каждый день
2) раз в неделю
3) раз в 3-6 месяцев
4) раз в год

7. К надежным характеристикам пароля не относится:
1) пароль должен состоять из 20 символов и больше
2) пароль должен включать в себя не только буквы
3) пароль должен включать в себя символы верхнего и нижнего регистров
4) пароль должен быть разный на каждом сайте (устройстве)

8. Виртуальная реальность это -
1) часть дополненной реальности
2) смоделированная реальность, в которой создается иллюзия присутствия пользователя в искусственном мире
3) дополнение реального мира, внося в него элементы искусственного.
4) состояние, в котором находится пользователь, когда одевает очки виртуальной реальности

9. Что из перечисленного не относится к технологическим процессам информатизации?
1) минитюризация
2) дигитализация
3) цифровизация
4) интеллектуализация

10. Прямое воздействие на психику и сознание людей в целях формирования нужных мнений и суждений – это..
1) информационная война
2) информационный терроризм
3) агрессивные слухи
4) запугивание

Ключ к промежуточной аттестации по информатике, 11 класс

1) 4

2) 3

3) 1

4) 2

5) 4

6) 3

7) 1

8) 2

9) 4

10) 2