

МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Департамент Смоленской области по образованию и науке
Муниципальное образование "Шумячский район" Смоленской области
МБОУ "Краснооктябрьская СШ"

РАССМОТРЕНО
ПЕДАГОГИЧЕСКИМ
СОВЕТОМ

Протокол №1 от «30» августа
2024 г.

УТВЕРЖДЕНО
И.о. директора

Александрова М.В.

Приказ №87 от «30» августа
2024 г.

РАБОЧАЯ ПРОГРАММА
по учебному курсу внеурочной деятельности
«Информационная безопасность»
10-11 класс

Составитель: Новикова В.Э.
учитель информатики

Пояснительная записка.

Нормативно правовые документы, на основе которых разработана данная программа

- Федерального закона от 29.12.12 И273-ФЗ (ред.13.07.2015) Об образовании в Российской Федерации»;
- Федерального государственного образовательного стандарта основного общего образования (Утвержден приказом Минобрнауки России от 17.12.2010 г. № 1897);
- Приказа Министерства образования и науки Российской Федерации от 17.12.2010 № 1897 «Об утверждении федерального государственного образовательного стандарта основного общего образования»;
- Приказа Министерства образования и науки Российской Федерации от 31.12.2015 № 1577 «О внесении изменений в федеральный государственный образовательный стандарт основного общего образования, утвержденный приказом Министерства образования и науки Российской Федерации от 17.12.2010 г. № 1577»;

Курс ориентирован на проведение уроков 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 социальных сетях, получения и передачи файлов, размещения личной информации в коллективных социальных сервисах.

Задачи курса по информационной безопасности детей:

1. 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;
2. создавать 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;
3. формировать отрицательное отношение ко всем проявлениям жестокости, насилия, нарушения прав личности, экстремизма во всех его формах в сети Интернет;
4. мотивировать обучающихся к осознанному поведению на основе понимания и принятия ими морально-правовых регуляторов жизни общества и государства в условиях цифрового мира;
5. 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 в Интернете как средoу созидания, а не разрушения человека и общества.

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. Курс рассчитан на 66 часов обучения, поддержан электронными ресурсами по каждой теме, ориентирован на работу обучающихся с документами в области законодательства Российской Федерации в сфере информационной безопасности.

Учебно - тематическое планирование разработано на основе учебного пособия по курсу для 10-11 классов. Пособие включает в себя практические работы по уровням «знать» и «применять», а также набор проектных заданий для выполнения в группах учащихся на компьютерах. К пособию для каждой темы на сайте издательства размещено электронное приложение с набором ссылок на материалы (документы, федеральные законы и ссылки к проектным работам) для использования на занятиях: <http://lbz.ru/metodist/authors/ib/10-11 .php>, возможно в демонстрационном режиме для использования педагогом при объяснении материала и организации обсуждений и дискуссий на занятиях.

Учебно-тематический план включает обязательный для изучения курса теоретический раздел 1 (Модули 1-4).

В рамках изучения курса обучающимся предложен дополнительный практический раздел 2 (Модуль 5), где представлены проектные работы, которые включают набор учебных практических работ и изучение открытого онлайн курса НОУ Интуит «Основы информационной безопасности» с прохождением

тестирования по итогам изучения курса. Раздел 2 курса учащиеся осваивают в компьютерном классе или в дистанционной форме.

Деятельность образовательного учреждения в обучении по направлению «Информационная безопасность» должна быть направлена на достижение обучающимися следующих **личностных результатов**:

- готовность и способность к самостоятельной, творческой и ответственной деятельности;
- навыки сотрудничества со сверстниками, детьми младшего возраста, взрослыми в образовательной, общественно полезной, учебно-исследовательской, проектной и других видах деятельности;
- готовность и способность к образованию, в том числе самообразованию, на протяжении всей жизни;
- сознательное отношение к непрерывному образованию как условию успешной профессиональной и общественной деятельности;
- эстетическое отношение к миру, включая эстетику научного и технического творчества;
- осознанный выбор будущей профессии и возможностей реализации собственных жизненных планов;
- отношение к профессиональной деятельности как возможности участия в решении личных, общественных, государственных, общенациональных проблем.

Метапредметными результатами освоения программы по направлению «Информационная безопасность» являются:

- умение самостоятельно определять цели и задачи деятельности; составлять планы; контролировать и корректировать их выполнение;
- умение продуктивно общаться и взаимодействовать в процессе совместной деятельности;
- владение навыками познавательной, учебно-исследовательской и проектной деятельности, способность и готовность к самостоятельному поиску методов решения практических задач;
- умение ориентироваться в различных источниках информации, критически оценивать и интерпретировать информацию;
- 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, информационной безопасности;

Предметными результатами освоения программы по направлению «Информационная безопасность» являются:

- развитие инженерного мышления;
- навыки работы с реальными программно-аппаратными комплексами;
- навыки оценивания уровня безопасности компьютерных систем;
- навыки обеспечения информационной безопасности личного пространства

Модуль	Параграфы в учебном пособии	Всего часов	Теоретические занятия	Практическая работа с ресурсами и программами на компьютере
<i>Раздел 1</i>				
Модуль 1. Правовые основы информационной безопасности	Глава 1 Понятия юридической ответственности за правонарушения в области информационной безопасности	5	2	3
1.1. Понятия юридической ответственности за правонарушения в области информационной безопасности	1. Основные документы в области информационной безопасности Российской Федерации 2. Информация как объект правовых отношений 3. Функции, принципы и виды юридической ответственности. 4. Субъективная и объективная стороны юридической ответственности	3	2	1
1.2. Контрольное занятие	Подготовка презентации по теме в группах учащихся	2		2
Модуль 2 Законодательство Российской Федерации о гражданско-правовой ответственности в сфере инфобезопасности	Глава 2. Гражданско-правовая ответственность за проступки в области информационной безопасности (защиты информации)	7	3	4
2.1 Законодательство Российской Федерации о гражданско-правовой ответственности	1. Общие положения законодательства Российской Федерации о гражданско-правовой ответственности 2. Порядок привлечения несовершеннолетних к гражданско-правовой ответственности за проступки в области информационной	3	2	1

	безопасности (защиты информации)			
2.2. Гражданско-правовая ответственность несовершеннолетних за проступки в области информационной безопасности (защиты информации)	1. Ответственность за проступок в области присвоение авторства (плагиат) 2. Ответственность за проступок за оскорбления, в том числе в социальных сетях	3	1	2
2.3.Контрольное занятие	Индивидуальный зачет	1		1
Модуль 3. Законодательство Российской Федерации об административной ответственности в сфере инфобезопасности	Глава 3. Административная ответственность за проступки в области информационной безопасности (защиты информации)	12	6	6
3.1.Понятие административной ответственности	1. Административное правонарушение. Основные понятия административного правонарушения 2. Особенности административной ответственности несовершеннолетних.	2	1	1
3.2 Административная ответственность несовершеннолетних граждан за проступки в области информационной безопасности (защиты информации).	1. Ответственность за проступок в области нарушения авторских прав на лицензионное программное обеспечение 2. Ответственность за проступок – за оскорбления, в том числе в социальных сетях 3. Ответственность за проступок - ложный вызов экстренных служб 4. Ответственность за проступок - пропаганду в Интернете наркотических и психотропных веществ 5. Ответственность за проступок –	9	5	4

	нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональные данные) 6. Ответственность за проступок – нарушение правил защиты информации 7. Ответственность за проступок – представление ложных сведений для получения документа, удостоверяющего личность гражданина (паспорта), либо других документов, удостоверяющих личность или гражданство 8. Ответственность за проступок – за подделку документов, штампов, печатей или бланков, их использование, передача, либо сбыт 9. Ответственность за проступок – нарушение правил производства, хранения, продажи и приобретения специальных технических средств, предназначенных для негласного получения информации			
3.3. Контрольное занятие	Индивидуальный зачет	1		1
Модуль 4 Законодательство Российской Федерации об уголовной ответственности в сфере инфобезопасности	Глава 4. Уголовная ответственность за правонарушения в области информационной безопасности (защиты информации)	14	7	7

4.1.Понятие уголовной ответственности	1. Уголовный кодекс Российской Федерации 2. Виды наказаний в области уголовной ответственности	2	1	1
4.2 Уголовная ответственность несовершеннолетних за преступления в области информационной безопасности (защиты информации)	1. Ответственность за преступления в области компьютерной информации и применения компьютеров 2. Ответственность за преступления в области присвоения авторства (плагиат) 3. Ответственность за преступления в области нарушения авторских прав на лицензионное программное обеспечение 4. Ответственность за преступления в области мошенничества (обмана) 5. Ответственность за преступления в области нарушения тайны переписки, телефонных переговоров или иных сообщений 6. Ответственность за преступления – за проведение скрытой (негласной) аудиозаписи 7. Ответственность за преступления – за заведомо ложное сообщение о теракте 8. Ответственность за преступления – за неприкосновенности частной жизни (тайна общения и творчества, дневников, личных бумаг) 9. Ответственность за	11	6	5

	преступления – за мошенничество в сфере компьютерной информации 10. Ответственность за преступления – за незаконное распространение порнографических материалов 11. Ответственность за преступления – за заведомо ложный донос			
4.3. Контрольное занятие	Индивидуальный зачет	1		1
Всего по разделу 1	Модули 1-4	33	18	15
Часы самостоятельной работы	Самостоятельная работа для индивидуальных зачетов и подготовки презентаций (предоставляется в компьютерной форме)	5		5
<i>Итого</i>	<i>Раздел 1</i>	<i>38</i>	<i>18</i>	<i>20</i>
<i>Раздел 2.</i>				
Модуль 5. Практика применения правил и норм информационной безопасности	Глава 5. Проектные задания	28	6	22
5.1. Проектная работа. Нормативные основы лицензионных соглашений	1. Лицензионное соглашение свободно го ПО Линукс 2. Как купить лицензию на платную антивирусн ую программу 3. Что такое СС лицензия 4. Обзор свободного антивирусного ПО и его возможности по антиспаму и шлюзованию	3	2	2
5.2. Проектная работа. Практика соблюдения норм инфобезопасности в личном информационном пространстве	1. Как задавать безопасный пароль. Настройки телефона, планшета для защиты от несанкционированно го доступа 2. Защита персональных данных. Обзор.	3	2	2

	Личный контент в облаке и система его защиты			
5.3. Онлайн-курс Основы информационной безопасности	Самостоятельная работа (по выбору учащихся)	15		15
5.4 Контрольное занятие.	Тест по онлайн курсу	1		1
Всего по разделу 2	Модуль 5	24	4	20
Резерв к разделу 2		4	2	2
<i>Итого</i>	<i>Раздел 2</i>	28	6	22
<u>Всего часов по курсу (разделы 1 и 2)</u>		66	24	42

Деятельность образовательного учреждения в обучении по направлению «Информационная безопасность» должна быть направлена на достижение обучающимися следующих **личностных результатов**:

- готовность и способность к самостоятельной, творческой и ответственной деятельности;
- навыки сотрудничества со сверстниками, детьми младшего возраста, взрослыми в образовательной, общественно полезной, учебно-исследовательской, проектной и других видах деятельности;
- готовность и способность к образованию, в том числе самообразованию, на протяжении всей жизни;
- сознательное отношение к непрерывному образованию как условию успешной профессиональной и общественной деятельности;
- эстетическое отношение к миру, включая эстетику научного и технического творчества;
- осознанный выбор будущей профессии и возможностей реализации собственных жизненных планов;
- отношение к профессиональной деятельности как возможности участия в решении личных, общественных, государственных, общенациональных проблем.

Метапредметными результатами освоения программы по направлению «Информационная безопасность» являются:

- умение самостоятельно определять цели и задачи деятельности; составлять планы; контролировать и корректировать их выполнение;
- умение продуктивно общаться и взаимодействовать в процессе совместной деятельности;
- владение навыками познавательной, учебно-исследовательской и проектной деятельности, способность и готовность к самостоятельному поиску методов решения практических задач;
- умение ориентироваться в различных источниках информации, критически оценивать и интерпретировать информацию;
- 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, информационной безопасности;

Предметными результатами освоения программы по направлению «Информационная безопасность» являются:

- развитие инженерного мышления;
- навыки работы с реальными программно-аппаратными комплексами;
- навыки оценивания уровня безопасности компьютерных систем;
- навыки обеспечения информационной безопасности личного пространства

Список источников информации:

- 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 безопасность. Правила безопасного Интернета. 2-4 классы: учебное пособие. — М.: БИНОМ. Лаборатория знаний, 2020. — 112 с.
3. Цветкова М. С., Якушина Е. В. Информационная безопасность. 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 безопасность. Кибербезопасность. 7-9 классы: учебное пособие. — М.: БИНОМ. Лаборатория знаний, 2020. — 64 с.
5. Цветкова М. С., Голубчиков С. В., Новиков В. К., Семибратов А. М., Якушина Е. В. Информационная безопасность: Правовые основы информационной безопасности. 10-11 классы: учебное пособие. — М.: БИНОМ. Лаборатория знаний, 2020. — 112 с.
6. Сайт электронного приложения к пособиям по информационной 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.m/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>
10. Открытый онлайн-курс «Безопасность в Интернете», «Академия Яндекс», компания Яндекс, URL: <https://academy.yandex.ru/events/online- courses/internet security/>