государственное бюджетное общеобразовательное учреждение
Самарской области средняя общеобразовательная школа с. Староганькино
муниципального района Похвистневский Самарской области

РАССМОТРЕНО	СОГЛАСОВАНО	УТВЕРЖДЕНО
на заседании МО Руководитель МО _____Иванова Н.Н. Протокол заседания №1 от 24 августа 2022 г	Заместитель директора по УВР _____Курманаева В.Е. 24 августа 2022 г	И.О. директора _____Иванова Н. Н. приказ №28/2 от 25 августа 2022 г.

РАБОЧАЯ ПРОГРАММА

ЭЛЕКТИВНОГО КУРСА ПО ИНФОРМАТИКЕ
«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»
(наименование учебного предмета (курса)

среднего общего образования (10-11 классы) (уровень образования)

базовый
(базовый/профильный уровень)

Составил : Ильин В.Л.

ГБОУ СОШ с. Староганькино,
2022 г.

ЭП
C=RU, O=ГБОУ СОШ с. Староганькино, CN=Иванова Н.Н., E=nadya_sg@mail.ru
008b7a2a74a6f1fa4

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Рабочая программа элективного курса по информатике «Информационная безопасность» для 10-11 классов составлена в соответствии с требованиями Федерального государственного образовательного стандарта среднего общего образования, на основе авторской программы «Информационная безопасность» 2-11 классы (автор – М.С. Цветкова) и основной образовательной программы среднего общего образования ГБОУ СОШ с. Староганькино муниципального района Похвистневский Самарской области

Содержание, последовательность изучения тем, объём рабочей программы полностью соответствует авторской программе.

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. 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.

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

Задачи курса по информационной безопасности детей:

- формировать понимание сущности и воспитывать необходимость принятия обучающимися таких ценностей, как человеческая жизнь, свобода, равноправие и достоинство людей, здоровье, опыт гуманных, уважительных отношений с окружающими;
- создавать педагогические условия для формирования правовой и информационной культуры обучающихся, развития у них критического отношения к информации, ответственности за поведение в сети Интернет и последствий 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 про- явлениям жестокости, насилия, нарушения прав личности, экстремизма во всех его формах в сети Интернет;
- мотивировать обучающихся к осознанному поведению на основе понимания и принятия ими морально - правовых регуляторов жизни общества и государства в условиях цифрового мира;
- научить молодых людей осознавать важность проектирования своей жизни и будущего своей страны — России в условиях развития цифрового мира, осознавать ценность ИКТ для

достижения высоких требований к обучению профессиям будущего в мире, принимать средства в Интернете как среду созидания, а не разрушения человека и общества.

Планируемые результаты освоения курса:

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, гражданского общества, многонационального российского на- рода, человечества.
- Быть социально активным, уважающим закон и правопорядок, 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.

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 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 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.

Также планируется достижение некоторых предметных результатов, актуальных для данного курса в интеграции с предметами: «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 результатов, 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.

Содержание программы

1. Правовые основы информационной безопасности

Понятия юридической ответственности за правонарушения в области информационной безопасности.

2. Законодательство Российской Федерации о гражданско - правовой ответственности в сфере инфобезопасности.

Законодательство Российской Федерации о гражданско - правовой ответственности. Гражданско - правовая ответственность несовершеннолетних за проступки в области информационной безопасности (защиты информации).

3. Законодательство Российской Федерации об административной ответственности в сфере инфобезопасности.

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

4. Законодательство Российской Федерации об уголовной ответственности в сфере инфобезопасности.

Понятие уголовной ответственности. Уголовная ответственность несовершеннолетних за преступления в области информационной безопасности (защиты информации).

5. Практика применения правил и норм информационной безопасности.

Проектная работа. Практика соблюдения норм инфобезопасности в личном информационном пространстве. **6. Онлайн - курс «Основы информационной безопасности».**

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.

К курсу разработано учебное пособие «Правовые основы информационной безопасности. 10–11 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 электронные документы и ресурсы для 10–11 классов http://lbz.ru/metodist/authors/ib/10-11.php

Курс может изучаться разделами в 10 и 11 по 1 часу в неделю, или за один год в 10 или 11 классах по 2 часа в неделю.

Контроль знаний умений и навыков.

В конце каждого модуля предусмотрено контрольное занятие. Аттестация учащихся проводится по системе **зачет/незачет.**

Тематическое планирование

Модуль	***Параграфы в учебном пособии***	***Всего часов***	***Теоретические занятия***	***Практическая работа на компьютере***
10 класс				
Раздел 1				
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	2. Основные документы в области ин формационной безопасности Российской Федерации 3. Информация как объект правовых отношений 4. Функции, принципы и виды юридической ответственности. 5. 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 безопасности (защиты информации)	3	2	1

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	Глава 3. Административная ответственность за проступки в области информационной безопасности (защиты информации)	***10***	***5***	***5***

инфобезопасности				
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 — 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	7	4	3

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)	***12***	***6***	***6***
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	9	5	4
	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 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***	***34***	***16***	***18***
11 класс				
Раздел 2				
Модуль 5. Практика применения правил и норм информационной безопасности	Глава 5. Проектные задания	***34***	***8***	***26***

5.1. Проектная работа. Нормативные основы лицензионных соглашений	1. Лицензионное соглашение свободного ПО Линукс. 2. Как купить лицензию на платную антивирусную программу. 3. Что такое СС лицензия. 4. Обзор свободного антивирусного ПО и его возможности по антиспаму и шлюзованию 5. Индивидуальный зачет. Защита проекта	7	3	4
5.2. Проектная работа. Практика соблюдения норм инфобезопасности в личном информационном пространстве	1. Как задавать безопасный пароль. Настройки телефона, планшета для защиты от несанкционированного доступа. 2. Защита персональных данных. Обзор. Личный контент в облаке и система его защиты. 3. Индивидуальный зачет. Защита проекта.	7	3	4
5.3. Самостоятельная дистанционная работа	Онлайн - курс «Основы информационной безопасности»	15		15
5.4 Контрольное занятие	Тест по онлайн - курсу	1		1
Всего по разделу 2	***Модуль 5***	***30***	***6***	***24***
Резерв к разделу 2		***4***	***2***	***2***
Всего часов по курсу (разделы 1 и 2)	За два года обучения (1 час в неделю) За один год обучения (2 часа в неделю)	***68***	***24***	***44***

ЛИТЕРАТУРА

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., Голубчиков С. В., Новиков В. К., Семибратов А. М., Якушина Е. В. Информационная безопасность: Правовые основы информационной безопасности. 10–11 классы : учебное пособие. — М.: Просвещение, 2021. — 112 с. 3. Сайт электронного приложения к пособиям по информационной безопасности, URL: http://lbz.ru/metodist/ authors/ib/
4. «Безопасный Билайн», компания Билайн, URL: http:// moskva.beeline.ru/customers/help/safe-beeline/
5. «Безопасность», компания МТС, URL: http://www.safety. mts.ru/ru/
6. «Безопасное общение», компания Мегафон, URL: http:// moscow.megafon.ru/bezopasnoe_obschenie/
7. «Памятка по безопасному общению», компания Мегафон, URL: http://moscow.megafon.ru/download/~msk/~moscow/ stopfraud/brochure.pdf
8. Открытый онлайн-курс «Безопасность в Интернете», «Академия Яндекс», компания Яндекс, URL: https:// academy.yandex.ru/events/online-courses/internet_security/