Министерство образования Иркутской области

Осинское муниципальное управление образованием

МБОУ "Приморская СОШ"

УТВЕРЖДЕНО
Приказом директора МБОУ
«Приморская СОШ»
_____
Малинкина М. В.
№78 от «30» августа 2024 г.

Малинкина Марина Владимировна

Подписано цифровой подписью: Малинкина Марина Владимировна
DN: c=RU, st=Иркутская область, l=п. Приморский, title=Директор школы, o=МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ "ПРИМОРСКАЯ СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА", 1.2.643.100.3=120B303837393837353033 8, 1.2.643.3.131.1.1=120C383530353030363937333833, email=primor-schooll@mail.ru, givenName=Марина Владимировна, sn=Малинкина, cn=Малинкина Марина Владимировна

Курс по внеурочной деятельности

«Цифровая гигиена и кибербезопасность»

для обучающихся 10–11 классов

Составил: Ситников Александр Викторович
Учитель информатики

п. Приморский 2024

Пояснительная записка

Нормативно правовые документы, на основе которых разработана данная программа

- Федерального закона от 29.12.12 №73-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.

Основными целями из учения курса **«**Цифровая гигиена**»** являются:

Обеспечение условий для профилактики негативных тенденций в информационной культуре учащихся, повышения защищенности детей от информационных рисков и угроз;

Формирование навыков своевременного распознавания онлайн рисков (технического, контентного, коммуникационного, потребительского характера и риска интернет зависимости).

Задачи программы:

✓ сформировать общекультурные навыки работы с информацией (умения, связанные с поиском, пониманием, организацией, архивированием цифровой информации и ее критическим осмыслением, а также с созданием информационных объектов с использованием цифровых ресурсов (текстовых, изобразительных, аудио и видео);

✓ создать условия для формирования умений, необходимых для различных форм коммуникации (электронная почта, чаты, блоги, форумы, социальные сети и др.) с различными целями и ответственного отношения к взаимодействию в современной информационно-телекоммуникационной среде;

✓ сформировать знания, позволяющие эффективно и безопасно использовать технические и программные средства для решения различных задач, в том числе использования компьютерных сетей, облачных сервисов и т.п.;

✓ сформировать знания, умения, мотивацию и ответственность, позволяющие решать с помощью цифровых устройств и интернета различные повседневные задачи, связанные с конкретными жизненными ситуациями, предполагающими удовлетворение различных потребностей;

✓ сформировать навыки по профилактике и коррекции зависимого поведения школьников, связанного с компьютерными технологиями и Интернетом.

Общая характеристика учебного курса

Курс «Цифровая гигиена» является важной составляющей работы с обучающимися, активно использующими различные сетевые формы общения (социальные сети, игры, пр.) с целью мотивации ответственного отношения к обеспечению своей личной безопасности, безопасности своей семьи и своих друзей. Кроме того, реализация курса создаст условиядлясокращения цифрового разрыва между поколениями и позволит родителям выступать в качестве экспертов, передающих опыт.

Описание места курса «Цифровая гигиена и Кибербезопасность» в учебном плане

В соответствии с учебным планом внеурочный курс **«**Цифровая гигиена**»** реализуется в 10-11 классе 2 года в объеме 34 часа в год, из расчета 1 час в неделю.

Формы текущего контроля и промежуточной аттестации

Форма текущего контроля: устный опрос; наблюдение за самостоятельной работой обучающегося, за его умением работать в группе сверстников; практическая работа; рефлексия в форме вербального проговаривания или письменного выражения своего отношения к теме, собственному участию в совместной работе

Годовая промежуточная аттестация проводится в форме тестирования.

Содержание внеурочного курса

Раздел 1. «Безопасность общения»

Тема 1. Общение в социальных сетях и мессенджерах. 1 час.

Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей и мессенджеров. Пользовательский контент.

Тема 2. С кем безопасно общаться в интернете. 1 час.

Персональные данные как основной капитал личного пространства в цифровом мире. Правила добавления друзей в социальных сетях. Профиль пользователя.

Тема 3. Пароли для аккаунтов социальных сетей. 1 час.

Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использование функции браузера по запоминанию паролей.

Тема 4. Безопасный вход в аккаунты. 1 час.

Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере с точки зрения безопасности личного аккаунта.

Тема 5. Настройки конфиденциальности в социальных сетях. 1 час.

Настройки приватности и конфиденциальности в разных социальных сетях. Приватность и конфиденциальность в мессенджерах.

Тема 6. Публикация информации в социальных сетях. 2 час.

Персональные данные. Публикация личной информации.

Тема 7. Кибербуллинг. 1 час.

Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать? Как не стать жертвой кибербуллинга. Как помочь жертве кибербуллинга.

Тема 8. Публичные аккаунты. 1 час.

Настройки приватности публичных страниц. Правила ведения публичных страниц.

Овершеринг.

Тема 9. Фишинг. 2 час.

Фишинг как мошеннический прием. Популярные варианты распространения фишинга. Отличие настоящих и фишинговых сайтов. Как защититься от фишеров в социальных сетях и мессенджерах.

Раздел 2. «Безопасность устройств»

Тема 1. Что такое вредоносный код. 1 час.

Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.

Тема 2. Распространение вредоносного кода. 1 час.

Способы доставки вредоносных кодов. Исполняемые файлы и расширения вредоносных кодов. Вредоносная рассылка. Вредоносные скрипты. Способы выявления наличия вредоносных кодов на устройствах. Действия при обнаружении вредоносных кодов на устройствах.

Тема 3. Методы защиты от вредоносных программ. 2 час.

Способы защиты устройств от вредоносного кода. Антивирусные программы и их характеристики. Правила защиты от вредоносных кодов.

Тема 4.Распространение вредоносного кода для мобильных устройств. 1 час.

Расширение вредоносных кодов для мобильных устройств. Правила безопасности при установке приложений на мобильные устройства. Раздел 3 «Безопасность информации»

Тема 1. Социальная инженерия: распознать и избежать. 1 час.

Приемы социальной инженерии. Правила безопасности при виртуальных контактах.

Тема 2. Ложная информация в Интернете. 1 час.

Цифровое пространство как площадка самопрезентации, экспериментирования и освоения различных социальных ролей. Фейковые новости. Поддельные страницы.

Тема 3. Безопасность при использовании платежных карт в Интернете. 1 час.

Транзакции и связанные с ними риски. Правила совершения онлайн покупок. Безопасность банковских сервисов.

Тема 4. Беспроводная технология связи. 1 час.

Уязвимость Wi-Fi-соединений. Публичные и непубличные сети. Правила работы в публичных сетях.

Тема 5. Резервное копирование данных . 2 час.

Безопасность личной информации. Создание резервных копий на различных устройствах.

Тема 6. Основы государственной политики в области формирования культуры информационной безопасности. 3 часа.

I. Планируемые результаты освоения курса внеурочной деятельности

Предметные:

- ✓ анализировать доменные имена компьютеров и адреса документов в интернете;
- ✓ безопасно использовать средства коммуникации,

- ✓ безопасно вести и применять способы самозащиты при попытке мошенничества,
- ✓ безопасно использовать ресурсы интернета.

Выпускник овладеет приемами безопасной организации своего личного пространства данных с использованием индивидуальных накопителей данных, интернет-сервисов и т.п.

Выпускник получит возможность овладеть:

- ✓ основами соблюдения норм информационной этики и права;
- ✓ основами самоконтроля, самооценки, принятия решений и осуществления осознанного выбора в учебной и познавательной
- ✓ деятельности при формировании современной культуры безопасности жизнедеятельности;
- ✓ использовать для решения коммуникативных задач в области безопасности жизнедеятельности различные источники информации, включая Интернет- ресурсы и другие базы данных.

Метапредметные.

Регулятивные универсальные учебные действия

В результате освоения учебного курса обучающийся сможет:

- ✓ идентифицировать собственные проблемы и определять главную проблему;
- ✓ выдвигать версии решения проблемы, формулировать гипотезы, предвосхищать конечный
- ✓ выбирать из предложенных вариантов и самостоятельно искать средства/ресурсы для решения задачи/достижения цели; составлять план решения проблемы (выполнения проекта, проведения исследования);
- ✓ описывать свой опыт, оформляя его для передачи другим людям в виде технологии решения практических задач определенного класса;
- ✓ оценивать свою деятельность, аргументируя причины достижения или отсутствия планируемого результата;
- ✓ принимать решение в учебной ситуации и нести за него ответственность.

Познавательные универсальные учебные действия.

В результате освоения учебного курса обучающийся сможет:

- ✓ выделять явление из общего ряда других явлений;
- ✓ определять обстоятельства, которые предшествовали возникновению связи между явлениями, из этих обстоятельств выделять
- ✓ строить рассуждение от общих закономерностей к частным явлениям и от частных явлений к общим закономерностям; излагать полученную информацию, интерпретируя ее в контексте решаемой задачи;
- ✓ самостоятельно указывать на информацию, нуждающуюся в проверке, предлагать и применять способ проверки достоверности информации;
- ✓ критически оценивать содержание и форму текста;
- ✓ определять необходимые ключевые поисковые слова и запросы.

Коммуникативные универсальные учебные действия.

В результате освоения учебного курса обучающийся сможет:

- ✓ строить позитивные отношения в процессе учебной и познавательной деятельности;
- ✓ договариваться о правилах и вопросах для обсуждения в соответствии с

поставленной перед группой задачей;

- ✓ целенаправленно искать и использовать информационные ресурсы, необходимые для решения учебных и практических задач с помощью средств ИКТ;
- ✓ использовать компьютерные технологии (включая выбор адекватных задаче инструментальных программно-аппаратных средств и сервисов) для решения информационных и коммуникационных учебных задач, в том числе: вычисление, написание писем, сочинений, докладов, рефератов, создание презентаций и др.;
- ✓ использовать информацию с учетом этических и правовых норм;
- ✓ создавать информационные ресурсы разного типа и для разных аудиторий, соблюдать информационную гигиену и правила информационной безопасности.

Личностные.

- ✓ осознанное, уважительное и доброжелательное отношение к окружающим людям в реальном и виртуальном мире, их позициям, взглядам, готовность вести диалог с другими людьми, обоснованно осуществлять выбор виртуальных собеседников;
- ✓ готовность и способность к осознанному выбору и построению дальнейшей индивидуальной траектории образования на базе ориентировки в мире профессий и профессиональных предпочтений, с учетом устойчивых познавательных интересов;
- ✓ освоенность социальных норм, правил поведения, ролей и форм социальной жизни в группах и сообществах;
- ✓ сформированность понимания ценности безопасного образа жизни; правила индивидуального и коллективного безопасного поведения в информационно-телекоммуникационной среде.

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 проявлениям жестокости, насилия, нарушения прав личности, экстремизма во всех его формах в сети Интернет;

— мотивировать обучающихся к осознанному поведению на основе понимания и принятия ими морально-правовых регуляторов жизни общества и государства в условиях цифрового мира;

— научить молодых людей осознавать важность проектирования своей жизни и будущего своей страны — России в условиях развития цифрового мира, 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.

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 35 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 Институт «Основы информационной безопасности» с прохождением тестирования по итогам изучения курса. Раздел 2 курса учащиеся осваивают в компьютерном классе или в дистанционной форме.

Требования к результатам освоения программы:

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

Тематическое планирование

№ п/п	Тема	Количество часов	Основное содержание	Характеристика основных видов учебной деятельности обучающихся
Тема 1. «Безопасность общения»				
1	Общение в социальных сетях и мессенджерах	1	Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей и мессенджеров. Пользовательский контент.	Выполняет базовые операции при использовании мессенджеров и социальных сетей. Создает свой образ в сети Интернет. Изучает историю и социальную значимость личных аккаунтов в сети Интернет.
2	С кем безопасно общаться в интернете	1	Персональные данные как основной капитал личного пространства в цифровом мире. Правила добавления друзей в социальных сетях. Профиль пользователя. Анонимные социальные сети.	Руководствуется в общении социальными ценностями и установками коллектива и общества в целом. Изучает правила сетевого общения.
3	Пароли для аккаунтов социальных сетей	1	Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использование функции браузера по запоминанию паролей.	Изучает основные понятия регистрационной информации и шифрования. Умеет их применить.
4	Безопасный вход в Аккаунты	1	Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере с точки зрения безопасности личного аккаунта.	Объясняет причины использования безопасного входа при работе на чужом устройстве. Демонстрирует устойчивый навык безопасного входа.
5	Настройки Конфиденциальности в социальных сетях	1	Настройки приватности и конфиденциальности в разных социальных сетях. Приватность и конфиденциальность в мессенджерах.	Раскрывает причины установки закрытого профиля. Меняет основные настройки приватности в личном профиле.
6	Публикация информации в социальных сетях	1	Персональные данные. Публикация личной информации.	Осуществляет поиск и использует информацию, необходимую для выполнения поставленных задач.

7	Кибербуллинг	1	Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать? Как не стать жертвой кибербуллинга. Как помочь жертве кибербуллинга.	Реагирует на опасные ситуации, распознает провокации и попытки манипуляции со стороны виртуальных собеседников.
8	Публичные аккаунты	1	Настройки приватности публичных страниц. Правила ведения публичных страниц. Овершеринг.	Решает экспериментальные задачи. Самостоятельно создает источники информации разного типа и для разных аудиторий, соблюдая правила информационной безопасности.
9	Фишинг	2	Фишинг как мошеннический прием. Популярные варианты распространения фишинга. Отличие настоящих и фишинговых сайтов. Как защититься от фишеров в социальных сетях и мессенджерах.	Анализ проблемных ситуаций. Разработка кейсов с примерами из личной жизни/жизни знакомых. Разработка и распространение чек- листа (памятки) по противодействию фишингу.
Тема 2. «Безопасность устройств»				
1	Что такое вредоносный код	1	Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.	Соблюдает технику безопасности при эксплуатации компьютерных систем. Использует инструментальные программные средства и сервисы адекватно задаче.
2	Распространение вредоносного кода	1	Способы доставки вредоносных кодов. Исполняемые файлы и расширения вредоносных кодов. Вредоносная рассылка. Вредоносные скрипты. Способы выявления наличия вредоносных кодов на устройствах. Действия при обнаружении вредоносных кодов на устройствах.	Выявляет и анализирует (при помощи чек- листа) возможные угрозы информационной безопасности объектов.
3	Методы защиты от вредоносных программ	2	Способы защиты устройств от вредоносного кода. Антивирусные программы и их характеристики. Правила защиты от вредоносных кодов	Изучает виды антивирусных Программ и правила их установки.
4	Распространение вредоносного кода для мобильных устройств	1	Расширение вредоносных кодов для мобильных устройств. Правила безопасности при установке приложений на мобильные устройства.	Разрабатывает презентацию, инструкцию по обнаружению, алгоритм установки приложений на мобильные устройства для учащихся более младшего возраста.

5.	Выполнение и защита индивидуальных и групповых проектов	3		Умеет работать индивидуально и в группе. Принимает позицию собеседника, понимая позицию другого, различает в его речи: мнение (точку зрения), доказательство (аргументы), факты; гипотезы, аксиомы, теории.
Тема 3 «Безопасность информации»				
1	Социальная инженерия: распознать и избежать	2	Приемы социальной инженерии. Правила безопасности при виртуальных контактах.	Находит нужную информацию в базах данных, составляя запросы на поиск. Систематизирует получаемую информацию в процессе поиска.
2	Ложная информация в Интернете	2	Цифровое пространство как площадка самопрезентации, экспериментирования и освоения различных социальных ролей. Фейковые новости. Поддельные страницы.	Определяет возможные источники необходимых сведений, осуществляет поиск информации. Отбирает и сравнивает материал по нескольким источникам.
3	Безопасность при использовании платежных карт в Интернете	1	Транзакции и связанные с ними риски. Правила совершения онлайн покупок. Безопасность банковских сервисов.	Приводит примеры рисков, связанных с совершением онлайн покупок (умеет определить источник риска). Разрабатываетвозможные варианты решения ситуаций, связанныхс рисками использования платежных карт в Интернете.
4	Беспроводная технология связи	1	Уязвимость Wi-Fi-соединений. Публичные и непубличные сети. Правила работы в публичных сетях.	Используя различную информацию,определяет понятия. Изучает особенности и стиль ведения личных и публичных аккаунтов.
5	Резервное копирование данных	2	Безопасность личной информации. Создание резервных копий на различных устройствах.	Создает резервные копии.

6	Основы государственной политики в области формирования культуры информационной Безопасности	2	Доктрина национальной информационной безопасности. Обеспечение свободы и равенства доступа к информации и знаниям. Основные направления государственной политики в области формирования культуры информационной безопасности.	Умеет привести выдержки из законодательства РФ: - обеспечивающего конституционное право на поиск, получение и распространение информации; Отражающего правовые аспекты защиты киберпространства.
7	Выполнение и защита индивидуальных и групповых проектов	3	Темы проектов Безопасность общения Безопасность устройств Безопасность общения	Уметь выполнять проекты Защита проектов
8	Годовая промежуточная аттестация	1	Тест Безопасность работы в интернете	Выполнение теста
9	Разбор типичных ошибок аттестационной работы	1	Анализ теста	Разбор ошибок
10	Итоговое занятие	1	Повторение	Повторение
	Итого	34		

План на 11 класс

Модуль	*Параграфы в учебном пособии*	*Всего часов*	*Теоретические занятия*	*Практическая работа с ресурсами*
Раздел 1				
Модуль 1. Правовые основы информационной безопасности	**Глава 1 Понятия юридической ответственности за правонарушения в области информационной безопасности**	***2***	**1**	**1**
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	2	1	1
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)**	**4**	**3**	**1**
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)	2	1	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	2	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)**	**11**	**8**	**3**

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	7	2
Модуль 4 Законодательство Российской Федерации об уголовной ответственности в сфере инфобезопасности	**Глава 4. Уголовная ответственность за правонарушения в области информационной безопасности (защиты информации)**	**8**	**4**	**4**
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	1. Ответственность за преступления в области компьютерной информации и применения	6	4	2

преступления в области информационной безопасности (защиты информации)	компьютеров 2 Ответственность за преступления в области присвоения авторства (плагиат); авторских прав на лицензионное программное обеспечение 3. Ответственность за преступления в области мошенничества (обмана) 4. Ответственность за преступления в области нарушения тайны переписки, телефонных переговоров или иных сообщений 5. Ответственность за преступления - за заведомо ложное сообщение о теракте 6. Ответственность за преступления - за мошенничество в сфере компьютерной информации			
Всего по разделу 1	**Модули 1-4**	**25**	**11**	**6**
Раздел 2.				
Модуль 5. Практика применения правил и норм информационной безопасности	**Глава 5. Проектные задания**	**10**	**5**	**5**
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 CC лицензия 4. Обзор свободного антивирусного ПО и его возможности по антиспаму и шлюзованию	7	4	3
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. Зашита персональных данных. Обзор. Личный контент в облаке и система его защиты	2	1	1
5.4 Контрольное занятие.	Тест по курсу	1		1
Всего по разделу 2	**Модуль 5**	**10**	**5**	**5**
Всего часов по курсу (разделы 1 и 2)	**За год обучения (1 час в неделю)**	**35**		

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. 10-11классы: 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.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

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