АДМИНИСТРАЦИЯ МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ
ГОРОДСКОГО ОКРУГА «ВОРКУТА»
МУНИЦИПАЛЬНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 13» г. ВОРКУТЫ
«ВОРКУТА» КАР КЫТШЛӦН МУНИЦИПАЛЬНӦЙ ЮКӦИСА АДМИНИСТРАЦИЯ
«13 №-а шор школа» Воркута карса муниципальной Велодан учреждение
169915, Республика Коми, г. Воркута,Ул. Суворова, д. 25-аТел.: (82151) 7-89-02
E-mail: school13rus@yandex.ru

РАССМОТРЕНА
школьным методическим объединением
учителей информационно-технологического цикла
Протокол № 1 от 31.08.2022

УТВЕРЖДАЮ
Директор МОУ «СОШ №13» г. Воркуты
_____ Шорохов А.А.
Приказ № 478 от 01.09.2022

Рабочая программа элективного курса «Компьютерная и информационная безопасность»

среднего общего образования
срок реализации программы 1 год

Рабочая программа учебного предмета составлена
в соответствии с Федеральным государственным образовательным стандартом
среднего общего образования
(в действующей редакции)

Составитель
Алексеева Людмила Петровна,
учитель информатики

г.Воркута
2022 год

Пояснительная записка

Рабочая программа элективного курса «Компьютерная и информационная безопасность» составлена в соответствии:

- с требованиями Федерального государственного образовательного стандарта среднего общего образования, утвержденного приказом Министерства образования и науки Российской Федерации от 17 мая 2012 г. № 413 (в действующей редакции); утвержденного приказом Министерства образования и науки Российской Федерации (в действующей редакции) и на основе

с учетом

- примерной основной образовательной программы среднего общего образования (одобрена решением федерального учебно-методического объединения по общему образованию (протокол от 28 июня 2016 г. №2/16-з).

программы элективных курсов по информатике “Компьютерная и информационная безопасность"" (http://www.referat-web.ru/referat56093.html).

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.

Сегодня уже ни у кого не вызывает сомнения тот факт, что XXI век – век информации и научных знаний. Развитие глобального процесса информатизации общества, охватывающего все развитые и многие развивающиеся страны мира, приводит к формированию новой информационной среды, информационного уклада и профессиональной деятельности. Однако при этом пропорционально возрастает уязвимость личных, общественных и государственных информационных ресурсов со стороны негативного воздействия средств инфомационно-коммуникационных технологий. Таким образом, мировое сообщество стоит перед глобальной социотехнической проблемой – проблемой обеспечения информационной безопасности. Под информационной безопасностью понимается область науки и техники, охватывающая совокупность программных, аппаратных и организационно-правовых методов и средств обеспечения безопасности информации при обработке, хранении и передаче с использованием современных информационных технологий. А так же под информационной безопасностью понимается защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры. Под угрозой информационной безопасности понимают потенциально возможное событие, действие, процесс или явление, которое может привести к нанесению ущерба чьим-либо интересам.

Решение проблемы безопасности вообще и информационной безопасности в частности невозможно без достаточного количества как высококвалифицированных профессионалов, так и квалифицированных пользователе, компетентных в сфере защиты информации. Задача подготовки таких специалистов является особенно актуальной ещё и потому, что одной из важнейших задач современности является борьба с компьютерной преступностью и кибертерроризмом. Спектр преступлений в сфере информационных технологий весьма широк, он варьируется от интернет-машенничества и до такой потенциально опасной деятельности, как электронный шпионаж и подготовка к террористическим актам.

В настоящее время достаточно свободно распространяются различные печатные издания, где описываются технологии совершения компьютерных преступлений; публикуются книги, освещающие приёмы атак на информационные системы. В Интернете представлено огромное количество сайтов, обучающих компьютерному взлому, проводятся форумы, виртуальные конференции и семинары по «повышению квалификации» и «обмену опытом» совершения компьютерных преступлений. Среди выявленных преступников, в отношении которых возбуждены дела за противоправные действия в сфере информационных технологий, свыше 75% составляет молодёжь. Всё это подчёркивает важность ещё одной задачи – активного противодействия вовлечению молодёжи в преступную среду и разработки активных методов

проведения воспитательной работы среди молодёжи. Очевидно, что насущной задачей современного образования становится разработка таких методов учебно-воспитательной работы, которые гармонично сочетают обучение современным информационным технологиям и формирование информационной культуры, высоких нравственных качеств, способствует выработке иммунитета к совершению неэтичных, противоправных действий в сфере информационных технологий.

Таким образом, можно считать актуальным и значительным старших классов изучение факультативного курса «Компьютерная и информационная безопасность» в образовательной области «Информатика». Курс ориентирован на подготовку подрастающего поколения к жизни и деятельности в совершенно новых условиях информационного общества, в котором вопросы обеспечения информационной безопасности личных, общественных и государственных информационных ресурсов особенно актуальны.

Количество часов за курс: 1 час в неделю, всего 35 учебных часа.

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.

Предметные результаты

Учащиеся научатся

– определять 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;

– 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 учебного курса

35 часа

1. Общие проблемы информационной безопасности.

Информация и информационные технологии. Актуальность проблемы обеспечения безопасности информационных технологий. Основные термины и определения. Субъекты информационных отношений, их интересы и безопасность. Конфиденциальность, целостность, доступность. Пути нанесения ущерба. Цели и объекты защиты.

2. Угрозы информационной безопасности.

Понятие угрозы. Виды проникновения или «нарушителей». Анализ угроз информационной безопасности. Классификация видов угроз информационной безопасности по различным признакам. Каналы утечки информации и их характеристика.

3. Вредоносные программы. Методы профилактики и защиты.

Общие сведения о вредоносных программах. Классификация по среде обитания, поражаемой операционной системе, особенностям алгоритма работы. Принципы функционирования, жизненный цикл и среда обитания компьютерных вирусов. Симптомы заражения и вызываемые вирусами эффекты. Полиморфные и стелс-вирусы. Вирусы-макросы для Microsoft Word и Microsoft Excel. Вирусы-черви. Профилактика заражения. Программные антивирусные средства. Определения и общие принципы функционирования фагов, детекторов, ревизоров, вакцин, сторожей. Структура антивирусной программы. Виды антивирусных программ.

4. Правовые основы обеспечения информационной безопасности.

Законодательство в информационной сфере. Виды защищаемой информации. Государственная тайна как особый вид защищаемой информации; система защиты государственной тайны; правовой режим защиты государственной тайны. Конфиденциальная информация. Лицензионная и сертификационная деятельность в области защиты информации. Основные законы и другие нормативно-правовые документы, регламентирующие деятельность организации в области защиты информации. Защита информации ограниченного доступа. Ответственность за нарушение законодательства в информационной сфере. Информация как объект преступных посягательств. Информация как средство совершения преступлений. Отечественные и зарубежные стандарты в области информационной безопасности.

5. Современные методы защиты информации в автоматизированных системах обработки данных.

Обзор современных методов защиты информации. Основные сервисы безопасности: идентификация и аутентификация, управление доступом, протоколирование и аудит. Криптографическое преобразование информации. История криптографии; простейшие шифры и их свойства. Принципы построения криптографических алгоритмов с симметричными и

несимметричными ключами. Электронная цифровая подпись. Контроль целостности; экранирование; анализ защищённости; обеспечение отказоустойчивости; обеспечение безопасного восстановления.

6. Технические и организационные методы защиты информации.

Технические средства охраны объектов (физическая защита доступа, противопожарные меры). Защита от утечки информации (перехвата данных, электростатических и электромагнитных излучений и др.). Технические средства противодействия несанкционированному съёму информации по возможным каналам её утечки. Организационные меры защиты. Определение круга лиц, ответственных за информационную безопасность, обеспечение надёжной и экономичной защиты. Требования к обслуживающему персоналу.

7. Защита информации в компьютерных сетях.

Примеры взломов сетей и веб-сайтов. Причины уязвимости сети Интернет. Цели, функции и задачи защиты информации в компьютерных сетях. Безопасность в сети Интернет. Методы атак, используемые злоумышлиниками для получения или уничтожения интересующей информации через Интернет. Способы отделения интрасети от глобальных сетей. Фильтрующий маршрутизатор, программный фильтр и т.д.

8. Проблемы информационно–психологической безопасности личности.

Определение понятия информационно-психологической безопасности. Основные виды информационно-психологических воздействий. Виртуальная реальность и её воздействие на нравственное, духовное, эмоциональное и физическое здоровье школьников. Игромания, компьютерные манипуляции, фишинг, киберугрозы и пропаганда других опасных явлений в Интернете. Способы Защиты от нежелательной информации в Интернете. Нравственно-этические проблемы информационного общества.

Тематическое планирование
11 класс (35 часов)

№	Темы	Количество часов	Виды деятельности учащихся
1	1. Общие проблемы информационной безопасности.	2	Слушание объяснений учителя. Объяснение и интерпретация наблюдаемых явлений
2	Угрозы информационной безопасности.	3	Слушание объяснений учителя. Просмотр и обсуждение учебных фильмов, презентаций, роликов Анализ проблемных учебных ситуаций
3	Вредоносные программы. Методы профилактики и защиты	3	Просмотр и обсуждение учебных фильмов, презентаций,

			роликов Выполнение работ практикума. Выполнение заданий по разграничению понятий.
4	Правовые основы обеспечения информационной безопасности.	5	Слушание объяснений учителя. Выполнение заданий по разграничению понятий. Просмотр и обсуждение учебных фильмов, презентаций, роликов
5	Современные методы защиты информации в автоматизированных системах обработки данных.	8	Просмотр и обсуждение учебных фильмов, презентаций, роликов Составление с помощью различных компьютерных средств обучения плана, тезисов, резюме, аннотации, аннотированного обзора литературы и др.
6	Технические и организационные методы защиты информации.	2	Решение экспериментальных задач
7	Защита информации в компьютерных сетях	5	Слушание объяснений учителя. Моделирование и конструирование. Выполнение заданий по разграничению понятий.
8	Проблемы информационно–психологической безопасности личности	7	Поиск информации в электронных справочных изданиях: электронной энциклопедии, словарях, в сети Интернет, электронных базах и банках данных
	Всего	35	