**МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**

Уланова Татьяна Алековна

Подписан: Уланова Татьяна Алековна
DN: C=RU, OU=и.о.директора, O=ГБОУ ООШ пос. Гражданский, CN=Уланова Татьяна Алековна, E=so_grazhdan_sch_krs@samara.edu.ru
Основание: я подтверждаю этот документ
Местоположение: 00c872063f816c2f92

**ГБОУ ООШ пос.Гражданский**

| РАССМОТРЕНО | СОГЛАСОВАНО | УТВЕРЖДЕНО |
|---|---|---|
| Руководитель МО | зам.директора по УВР | и.о.директора |
| _____ | _____ | _____ |
| Жданова Е.Н. | Ерхова Г.М. | Уланова Т.А. |
| Протокол 1 от «26» августа 2023 г. | от «30» августа 2023 г. | Приказ №108-од от «30» августа 2023 г. |

**РАБОЧАЯ ПРОГРАММА**

Предмет (курс) «Информационная безопасность или на расстоянии одного вируса» Класс 8

Общее количество часов по учебному плану 34 часа.

Составлена в соответствии с Примерной рабочей программой пособия Наместникова М.С. «Информационная безопасность, или на расстоянии одного вируса»

Учебник:

- Автор: Наместникова М.С
- Наименование: . «Информационная безопасность, или на расстоянии одного вируса 7-9 классы
- Издательство, год. « Просвещение 2019 год».

**Пояснительная записка**

Рабочая программа элективного курса «Информационная безопасность» предназначена для учащихся 8 класса. Курс рассчитан на 34 часа учебного времени в год. Имеет тесную связь с учебной дисциплиной «Информатика».

В соответствии с ФГОС основного общего образования РФ образовательная деятельность учебного учреждения основывается на системно-деятельностном подходе, который обеспечивает:

- формирование готовности к саморазвитию и непрерывному образованию;
- проектирование и конструирование социальной среды развития обучающихся в системе образования;
- активную учебно-познавательную деятельность обучающихся;
- построение образовательного процесса с учётом индивидуальных возрастных, психологических и физиологических особенностей обучающихся.

Именно этот подход позволяет достичь реализации целей образовательного стандарта и сформировать личностные характеристики выпускника, соответствующие «портрету выпускника основной школы».

Изучение элективного курса «Информационная безопасность» позволяет гармонично сочетать обучение современным информационным технологиям и формирование информационной культуры, высоких нравственных качеств, способствует выработке иммунитета к совершению неэтичных, противоправных действий в сфере информационных технологий.

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.

**Структура документа**

Рабочая программа включает разделы: пояснительная записка; структура и содержание курса; учебно-тематический план; требования к уровню подготовки обучающихся; литература.

**ПОЯСНИТЕЛЬНАЯ ЗАПИСКА**

**Актуальность**

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 информационно-коммуникационных технологий. Таким образом, мировое сообщество стоит перед глобальной социотехнической проблемой – проблемой обеспечения информационной безопасности.

Решение проблемы безопасности вообще и информационной безопасности в частности невозможно без достаточного количества как высококвалифицированных профессионалов, так и квалифицированных пользователей, компетентных в сфере защиты информации.

Данный курс преследует следующие **цели:**

 Овладение учащимися умениями: профилактики, защиты программного обеспечения; обнаружения и удаления компьютерных вирусов; защиты информации в автоматизированных системах обработки данных, в глобальной сети Интернет.

 Приобретение учащимися опыта по предупреждению и нейтрализации негативного воздействия информационных угроз на людей и программно-технические комплексы; опыта информационной деятельности в сферах обеспечения защиты информации, актуальных на рынке труда.

 Приобретения учащимися опыта создания, редактирования, оформления, сохранения, передачи информационных объектов различного типа с помощью современных программных средств; коллективной реализации информационных проектов, преодоления трудностей в процессе проектирования, разработки и реализации учебных проектов.

Перед данным элективным курсом ставятся следующие **задачи:**

*образовательные:*

 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 вычислительной технике и в системах связи;

*развивающие:*

 повышение интереса учащихся к изучению информатики;
 приобретение учащимися навыков самостоятельной работы с учебной, научно-популярной литературой и материалами сети Интернет;
 развитие у учащихся способностей к исследовательской деятельности;

*воспитательные:*

 воспитание у учащихся культуры в области применения ИКТ в различных сферах современной жизни;
 воспитание у учащихся чувства ответственности за результаты своего труда, используемые другими людьми;
 воспитание у учащихся умения планировать, работать в коллективе;
 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.

**Формы учебных занятий**

При реализации образовательной программы формы учебных занятий могут быть самыми разнообразными, все зависит от тех целей и задач, которые ставит на конкретном уроке преподаватель. Это могут быть:

1. классический урок,
2. лекционно-семинарские или лекционно-практические занятия,
3. интегрированный урок,
4. проектные занятия, творческая мастерская,
5. нетрадиционные уроки,
6. лабораторные работы

**Формы обучения:** индивидуальная, фронтальная, парная, групповая, коллективная.

**Методы обучения:** объяснительно-иллюстративный, проблемный, репродуктивный, частично-поисковый, исследовательский.

Обсуждение результатов лабораторных работ с точки зрения оценки их действительности; защита собственных проектов и обсуждение проектов своих товарищей.

**Формы контроля достижений учащихся**

Работа учащихся оценивается учителем, одноклассниками, дается самооценка. Учитель оценивает отчеты по лабораторным работам, рефераты. Лучшие работы заслушиваются на любом занятии. Учитель и учащиеся оценивают участие в подготовке и проведении конференций, вечеров, семинаров.

Ученик может предварительно контролировать себя, для этого критерии

оценки учитель должен сообщить перед началом работы.

**Прогнозируемый результат**

Участие в конкурсах, конференциях; выбор учащимися агротехнического профиля дальнейшего обучения.

**Обучающиеся должны знать:**

 основные понятия и определения из области обеспечения информационной безопасности;
 методы и средства борьбы с угрозами информационной безопасности;
 классификацию вредоносных программ и их влияние на целостность информации; порядок заражения файлов;
 методы проведения профилактики, защиты и восстановления пораженных вредоносными программами объектов;
 нормативные руководящие документы, касающиеся защиты информации, существующие стандарты информационной безопасности;
 принципы выбора пароля, аппаратные и программные средства для аутентификации по паролю;
 основные понятия криптографических методов защиты информации, механизмы цифровой электронной подписи;
 существующие программные продукты, предназначенные для защиты электронного обмена данными в Интернете, способы отделения интрасети от глобальных сетей;
 нормы информационной этики и права.

**Учащиеся должны уметь:**

 объяснять необходимость изучения проблемы информационной безопасности;
 применять методы профилактики и защиты информационных ресурсов от вредоносного программного обеспечения;
 восстанавливать повреждённую информацию;
 соблюдать права интеллектуальной собственности на информацию;
 применять методы ограничения, контроля, разграничения доступа, идентификации и аутентификации;
 использовать современные методы программирования для разработки сервисов безопасности;
 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;
 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;
 представлять результаты учебных исследовательских проектов с использованием информационно-коммуникационных технологий.

**Система оценивания**

Предполагается текущий и итоговый контроль.
Текущий контроль в форме:
- устные ответы,
- обсуждения,
- отчеты по лабораторным работам,
- представление сообщений, рефератов, презентаций.

Итоговый контроль в форме защиты проектов.
Результаты обучения оцениваются по пятибалльной системе. В течение всего периода обучения предполагается самооценка и оценка преподавателя. Итоговая оценка преподавателя согласуется с самооценкой учащегося.

**Материально-техническая база**

1. Персональные компьютеры, объединенные в локальную сеть с выделенным сервером и высокоскоростным доступом в Internet
1. Операционная система Linux, Windows XP/7/8.
2. Интегрированный пакет Microsoft Office 2007/2010.

**СТРУКТУРА И СОДЕРЖАНИЕ КУРСА (34 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 безопасноговосстановления.

*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.

**Учебно-тематический план**

# Календарно-тематическое планирование на учебный год: 2020/2021

**Вариант:** Информационная безопасность 8 класс 2020

**Общее количество часов:** 34

| № урока | Тема урока | Кол-во часов |
|---|---|---|
| *Раздел 1: Безопасность общения. - 14 ч* | | |
| 1. | Общение в социальных сетях и мессенджерах. | 1 |
| 2. | С кем безопасно общаться в Интернете. | 1 |
| 3. | Пароли для аккаунтов социальных сетей. | 1 |
| 4. | Безопасный вход в аккаунты. | 1 |
| 5. | Настройки конфиденциальности в социальных сетях. | 1 |
| 6. | Публикация информации в социальных сетях. | 1 |
| 7. | Кибербуллинг. | 1 |
| 8. | Публичные аккаунты. | 1 |
| 9. | Фишинг. | 1 |
| 10. | Тест 1 | 1 |
| 11. | Выполнение и защита индивидуальных проектов. | 1 |
| 12. | Выполнение и защита индивидуальных проектов 2 | 1 |
| 13. | Выполнение и защита индивидуальных проектов 3 | 1 |
| 14. | Выполнение и защита индивидуальных проектов 4 | 1 |
| *Раздел 2: Безопасность устройств. - 9 ч* | | |

| | | |
|---|---|---|
| 1. | Что такое вредоносный код. | 1 |
| 2. | Распространение вредоносного кода. | 1 |
| 3. | Методы защиты от вредоносных программ. | 1 |
| 4. | Распространение вредоносного кода для мобильных устройств. | 1 |
| 5. | Тест 2. | 1 |
| 6. | Выполнение и защита индивидуальных проектов 1. | 1 |
| 7. | Выполнение и защита индивидуальных проектов 2. | 1 |
| 8. | Выполнение и защита индивидуальных проектов 3. | 1 |
| 9. | Выполнение и защита индивидуальных проектов 4. | 1 |
| *Раздел 3: Безопасность и информация. - 9 ч* | | |
| 1. | Социальная инженерия: распознать и избежать. | 1 |
| 2. | Ложная информация в Интернете. | 1 |
| 3. | Беспроводная технология связи. | 1 |
| 4. | Резервное копирование данных. | 1 |
| 5. | Тест 3. | 1 |
| 6. | Выполнение и защита индивидуальных проектов 1. | 1 |
| 7. | Выполнение и защита индивидуальных проектов 2. | 1 |
| 8. | Выполнение и защита индивидуальных проектов 3. | 1 |
| 9. | Выполнение и защита индивидуальных проектов 4. | 1 |
| *Раздел 4: Повторение. - 2 ч* | | |
| 1. | Тема: "Безопасность общения и безопасность информации". | 1 |
| 2. | Тема: "Безопасность устройств". | 1 |

**ЛИТЕРАТУРА И СРЕДСТВА ОБУЧЕНИЯ**

1. Грушо А.А., Тимонина Е.Е. Теоретические основы защиты информации. – М.: Издательство Агентства «Яхтсмен», 1996.
2. Девянин П.Н., Михальский О.О., Правиков Д.И., Щербаков А.Ю. Теоретические основы компьютерной безопасности. – М.: Радио и связь, 2000.
3. Казарин О.В. Безопасность программного обеспечения компьютерных систем. Монография. – М.: МГУЛ, 2003. – 212 с.
4. Новиков А.А., Устинов Г.Н. Уязвимость и информационная безопасность телекоммуникационных технологий: Учебное пособие. – М. «Радио и связь» 2003.
12
5. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. –МЦНМО, 2003.
6. Введение в криптографию. – Сб. под ред. В.В.Ященко. МЦНМО, 1999.