Рассмотрено на заседании
ШМО
руководитель
_____/Р.В.Галимова/
Протокол № 10
от «28» августа 2023г.

Согласовано
заместитель директора
по УР
_____/Л.А.Гордеева/
«23» августа 2023г.

«Утверждаю»
Директор МБОУ КСШ №3
_____/Д.Х.Ганиева/
Приказ № 456/23
от «28» августа 2023г.

Информационная безопасность
элективный курс для учащихся 11 класса
рассчитан на 34 часа

Разработала Галимова Роза Викторовна,
учитель информатики
высшей квалификационной категории

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.

Цель курса: овладение учащимися навыков профилактики и защиты программного обеспечения и информации;

Задачи курса:

• Систематизировать подходы к изучению материала;

• Сформировать у учащихся единую систему понятий, связанных с созданием, получением, обработкой, интерпретацией и хранением информации;

• Показать основные приёмы эффективного использования информационных ресурсов Интернет;

• Приобрести практические навыки в работе с современными ПК и программными средствами;

• Приобрести опыт в предупреждении и нейтрализации угроз информации;

- Научиться создавать и реализовывать информационные проекты.

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.

Данный элективный курс поможет получить актуальные, на сегодняшний день, знания, умения и навыки в современных информационных технологиях.

Информационная безопасность — защита конфиденциальности, целостности и доступности информации. Защита информации – комплекс мероприятий, направленных на обеспечение информационной безопасности.

Ожидаемые результаты курса

После прохождения курса, должен быть достигнут следующий перечень знаний, умений и навыков учащихся.

Учащиеся 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 информационныхресурсов от вредоносного программного обеспечения;
- восстанавливать повреждённую информация;
- соблюдать права интеллектуальной собственности н аинформацию;
- применять методы ограничения, контроля, разграничениядоступа, идентификации и аутентификации;
- использовать современные методы программирования дляразработки сервисов безопасности;
- производить простейшие криптографические преобразованияинформации;
- планировать организационные мероприятия, проводимые призащите информации;

- применять методы защиты информации в компьютерных сетях;
- различать основные виды информационно-психологических воздействий в виртуальной реальности;
- соблюдать требования информационной безопасности, этики иправа;
- 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.

Курс служит средством внутри профильной специализации в области информатики и информационных технологий, что способствует созданию дополнительных условий для построения индивидуальных образовательных траекторий учащихся классов информационно-технологического профиля. Курс рассчитан на 34 часа и изучается в течение одного учебного года по 1 часу в неделю в 11 классе.

Содержание курса

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

№	Наименование разделов программ	Количество часов	Электронные(цифровые ресурсы)
1	Общие проблемы информационной безопасности	2	https://kpolyakov.spb.ru
2	Угрозы информационной безопасности	4	https://kpolyakov.spb.ru
3	Правовые основы	6	https://kpolyakov.spb.ru

	обеспечения информационной безопасности		
4	Современные методы защиты информации в автоматизированных системах обработки данных	8	https://kpolyakov.spb.ru
5	Технические и организационные методы хранения информации	2	https://kpolyakov.spb.ru
6	Защита информации в компьютерных сетях. Проблемы информационно–психологической безопасности личности	12	https://kpolyakov.spb.ru