МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Министерство образования и науки Пермского края
Управление образования администрации
Пермского муниципального округа
МАОУ «Кондратовская средняя школа «Сфера»

СОГЛАСОВАНО

Педагогическим советом МАОУ «Кондратовская средняя школа «Сфера»

Протокол №1
от «07» 11 2024 г.

УТВЕРЖДЕНО

Директор

_____ Кетова В.Д.

Приказ № 15
от «07» 11 2024 г.

РАБОЧАЯ ПРОГРАММА

по курсу дополнительного образования

«Информационная безопасность компьютерных сетей»

для 10-11 класса

Составитель Кифер Диана Александровна,
педагог дополнительного образования

2024г.

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Одно из основных мест в системе предпрофильной подготовки занимают курсы дополнительного образования у старшеклассников. В современном мире, где люди проводят за компьютером и в сети достаточно много времени, особо важным становится владеть знаниями о существующих угрозах в компьютерных сетях и о методах борьбы с ними.

Предложенный курс преследует такие цели, как:

- овладение учащимися навыков профилактики и защиты программного обеспечения и информации;
- приобретения опыта в предупреждении и нейтрализации угроз информации;
- соблюдение правовых и этических норм при работе в сети;
- научиться создавать и реализовывать информационные проекты.

Перед данным элективным курсом ставятся следующие задачи:

- Познакомить учащихся, с понятием информационной безопасности компьютерных сетей;
- Познакомить с правовыми основами в области ИБКС;
- Познакомить учащихся с тем, как устроены различные сетевые протоколы с точки зрения безопасности.
- Научить анализировать трафик, перехваченный в проводных и беспроводных сетях,
- Познакомить с современными методами защиты информации;
- Познакомить с проблемами информационно–психологической безопасности личности в компьютерных сетях.

Содержание курса

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 для старших классов изучение курса «Информационная безопасность компьютерных сетей».

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.

Курс служит средством внутри **профильной специализации** в области информатики и информационных технологий, что способствует созданию дополнительных условий для построения индивидуальных образовательных траекторий.

Курс рассчитан на 34 часа и изучается в течение одного учебного года по 1 часу в неделю в 11 классе.

Для успешного изучения курса «Информационная безопасность компьютерных сетей» необходимы базовые знания, полученные учащимися при изучении информатики и информационных технологий.

Учащиеся должны знать:

- свойства алгоритмов и основные алгоритмические структуры;
- основные конструкции языка программирования;
- назначение и области использования основных технических средств информационных и коммуникационных технологий и информационных ресурсов;
- базовые принципы организации и функционирования компьютерных сетей.

Учащиеся должны уметь:

- составлять программы на языке программирования;
- проводить статистическую обработку данных с помощью компьютера;
- строить таблицы, графики, диаграммы;
- представлять информацию в виде мультимедийных объектов с системой ссылок;
- подготавливать доклады и проводить выступления;
- участвовать в коллективном обсуждении без использования современных программных и аппаратных средств коммуникаций и с их использованием.

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 информационных ресурсов от вредоносного программного обеспечения;
- восстанавливать повреждённую информация; 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.

Программа курса

1. *Общие проблемы информационной безопасности. (2ч)*

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.(4ч)*

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

3. *Современные методы защиты информации в автоматизированных системах обработки данных.(8ч)*

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.

4. *Технические и организационные методы защиты информации.(3ч)*

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.

5. *Защита информации в компьютерных сетях.(2ч)*

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 злоумышленниками для получения или уничтожения интересующей информации через Интернет. Способы отделения интрасети от глобальных сетей. Фильтрующий маршрутизатор, программный фильтр и т.д.

6. *Проблемы информационно–психологической безопасности личности.(4ч)*

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.

7. *Правовые основы обеспечения информационной безопасности.(11ч)*

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.

Календарно-тематическое планирование

№	Тема	Кол-во часов
	Тема 1: Общие проблемы информационной безопасности – 2 часа	
1.	Основные понятия информационной безопасности. Актуальность проблемы обеспечения безопасности ИТ.	1
2.		1
	Тема 2: Угрозы информационной безопасности – 4 часа	
3.	Понятие угрозы информационной безопасности. Классификация видов угроз информационной безопасности по различным признакам.	1
4.		1
5.	Методы защиты компьютеров от вредоносных программ. Восстановление информации.	1
6.	Практическая работа: Методы защиты компьютеров от вредоносных программ. Восстановление информации.	1
	Тема 3: Современные методы защиты информации в автоматизированных системах обработки данных – 8 часов.	
7.	Основные сервисы безопасности. Идентификация и аутентификация.	1
8.		1
9.	Управление доступом. Протоколирование и аудит. Криптографическая защита.	1
10.	Практическая работа: Управление доступом. Протоколирование и аудит. Криптографическая защита.	1
11.	Принципы построения криптографических алгоритмов с симметричными и несимметричными ключами.	1
12.	Практическая работа: Принципы построения криптографических алгоритмов с симметричными и несимметричными ключами.	1
13.	Контроль целостности; экранирование; анализ защищённости.	1
14.		1
	Тема 4: Технические и организационные методы защиты информации. – 3 часа	
15.	Технические средства защиты информации. Организационные меры защиты.	1
16.		1
17.		

	Тема 5: Защита информации в компьютерных сетях – 2 часа	
18.	Защита информации в компьютерных сетях. Безопасность в сети Интернет	1
19.	Практическая работа: Фильтрующий маршрутизатор, программный фильтр, системы типа FireWall (брандмауэр, экранирующий фильтр) и т.д	1
	Тема 6: Проблемы информационно–психологической безопасности личности –4 часов.	
20.	Виртуальная реальность и её воздействие на нравственное, духовное, эмоциональное и лекция физическое здоровье школьников	1
21.	Способы защиты от нежелательной информации в Интернете.	1
22.	Защита персональных данных (ПД).	1
23.	Практическая работа по теме: Защита персональных данных (ПД).	1
	Тема 7: Правовые основы обеспечения информационной безопасности – 11 часов	
24.	Законодательство в области защиты информации.	1
25.		1
26.	Преступление и наказание в сфере информационных технологий.	1
27.	Практическая работа: Преступление и наказание в сфере информационных технологий.	1
28.	Отечественные и зарубежные стандарты в области	1
29.	информационных технологий.	1
30.	Работа над проектом «Перспективные направления в области	1
31.	обеспечения информационной безопасности».	1
32.		1
33.		1
34.	Итоговое занятие. Защита проектов.	1
	ИТОГО	34

Литература

1. Гостехкомиссия России. Руководящий документ: Защита от несанкционированного доступа к информации. Термины и определения. – М.: ГТК 1992.

2. Грушо А.А., Тимонина Е.Е. Теоретические основы защиты информации. – М.: Издательство Агентства «Яхтсмен», 1996.

3. Девянин П.Н., Михальский О.О., Правиков Д.И., Щербаков А.Ю. Теоретические основы компьютерной безопасности. – М.: Радио и связь, 2000.

4. Казарин О.В. Безопасность программного обеспечения компьютерных систем. Монография. – М.: МГУЛ, 2003. – 212 с.

5. Новиков А.А., Устинов Г.Н. Уязвимость и информационная безопасность телекоммуникационных технологий: Учебное пособие. – М. «Радио и связь» 2003.

6. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. – МЦНМО, 2003.

7. Введение в криптографию. – Сб. под ред. В.В.Ященко. МЦНМО, 1999.

8. Спесивцев А.В., Вегнер В.А., Крутяков А.Ю. и др. Защита информации в персональных ЭВМ. – М. «Радио и связь», Веста, 1992.

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП

Сертификат 722671968566237128169706768058107758750791459327

Владелец Кетова Валерия Дмитриевна

Действителен С 08.11.2024 по 08.11.2025