МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Министерство образования Оренбургской области

Управление образования Абдулинского городского округа

МБОУ "Искринская ООШ"

РАССМОТРЕНО	СОГЛАСОВАНО	УТВЕРЖДЕНО
на заседании ШМО учителей естественно-научного цикла	заместитель директора по УВР	директор МБОУ "Искринская ООШ"
Шамакина Л.Н.	Лобкарёва Л.Н.	Кожаева Н.Л.
Приказ №1 от «30» августа 2023 г.	Приказ №1 от «30» августа 2023 г.	Приказ № 1 от «30» августа 2023 г.

РАБОЧАЯ ПРОГРАММА

элективного курса «Основы информационной безопасности при работе в телекоммуникационных сетях»

для обучающихся 9 класса.

п.Искра 2023

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Программа элективного курса разработана на основе программы элективного курса «Основы информационной безопасности при работе в телекоммуникационных сетях» И.А. Калинина ,Н.Н. Самылкиной, рассчитанную на 7 часов.

Цель курса: освоение основных знаний и формирование умений по обеспечения информационной безопасности при работе сети.

Задачи курса. Для реализации поставленной цели необходимо решение следующих задач:

- Освоение учащимися основных понятий информационной безопасности, а также формирование умений по устранению и уменьшению последствий ее нарушения;
- Формирование умений работать с основными классами программных средств для обеспечения информационной установки при работе в сети и практических навыков их установки, настройки и использования на конкретных примерах;
- Ознакомление учащихся с методами контроля источников информации;
- Формирование навыков построения персонального защитного комплекса для одиночного компьютера;
- Воспитание уважительного отношения к другим пользователям сети, соблюдения правил сетевого этикета.

Для успешного изучения данного элективного курса необходимо обладать следующей подготовкой, полученной в ходе изучения информатики и информационных технологий основной школе.

Учащиеся должны:

- Обладать знаниями, составляющими основу научных представлений об информации, информационных процессах, системах, технологиях и моделях;
- Уметь работать с различными идами информации с помощью компьютера и других средств информационных технологий (ИКТ), организовать собственную информационную деятельность и планировать ее результаты;
- Стремиться развивать сои познавательные интересы, интеллектуальные и творческие способности при помощи средств ИКТ;
- Ответственно относиться к информации с учетом правовых и этических аспектов ее распространения, избирательного отношения к полученной информации;
- Обладать навыками применения средств ИКТ в повседневной жизни, при выполнении индивидуальных и коллективных проектов в учебной деятельности

При этом предполагается, что в соответствии со стандартом среднего (полного) общего образования по информатике и ИКТ профильного уровня в разделе «Средства ИКТ» школьником были изучены следующие темы:

- Архитектура компьютеров и компьютерных сетей. Программная и аппаратная организация компьютеров и компьютерных систем. Виды программного обеспечения. Операционные системы. Понятие о системном администрировании.
- Безопасность, гигиена, эргономика, ресурсосбережение, технологические требования при эксплуатации компьютерного рабочего места. Типичные неисправности и трудности в использовании ИКТ. Комплектация компьютерного рабочего места соответствии с целями его использования.
- Оценка числовых параметров информационных объектов и процессов, характерных для выбранной области деятельности.
- Профилактика оборудования.

Также предполагается, что в разделе «Телекоммуникационные технологии» были изучены следующие вопросы:

- Представления о средствах телекоммуникационных технологий: электронная почта, чат, телеконференции, форумы, телемосты, интернет-телефония. Специальное программное обеспечение средств телекоммуникационных технологий. Использование средств телекоммуникаций коллективной деятельности.
- Технологии и средства защиты информации в глобальной и локальной компьютерной сети от разрушения, несанкционированного доступа. Правила подписки на антивирусные программы и их настройка на автоматическую проверку сообщений.
- Инструменты создания информационных объектов для сети Интернет. Методы и средства создания и сопровождения сайта.

Программа предлагаемого элективного курса (курса по выбору учащихся) ориентирована на развитие знаний и умений по обеспечению информационной безопасности при работе на персональном компьютере в сети, полученных в основной школе и в ходе изучения определенных тем курса информатики профильного уровня. Данный курс предназначен для тех, кто определил информатику как сферу своих будущих профессиональных интересов в качестве основного направления, поэтому его содержание представляет собой самостоятельный модуль, изучаемый в старшей школе.

Курс «Основы информационной безопасности при работе в телекоммуникационных сетях», опираясь на ранее изученный школьниками материал, призван разить наиболее важные вопросы технологии и средств защиты информации сети, а также сформировать целостную, пригодную к практическому использованию систему понятий данной области деятельности. Курс позволит учащимся освоить необходимые практические навыки.

Предлагаемый курс может носить общий характер для проведения занятий по выбору в группах естественнонаучного, технологического или математического профиля. Его изучение возможно и случае, если курс информатики в старшей школе изучается на базовом уровне. Тогда наилучшим вариантом будет увеличение количества учебных часов, отводимых на этот электив, и включение в него необходимых тем из вышеперечисленных разделов.

При изучении данного элективного курса предполагается использование демонстрационных средств, по возможности – максимально современных, и доступ к системам обновления для обеспечения максимальной актуальности материала.

ОСНОВНОЕ СОДЕЖАНИЕ КУРСА

1. Базовые определения (1 час).

Аспекты безопасности (целостность, доступность, конфиденциальность), понятия уязвимости, угрозы, атаки, эксплуатации уязвимости, инцидента. Основы стратегии предупреждения нарушений (резервирование, распознавание, устранение уязвимостей, уменьшение количества точек взаимодействия). Примеры инцидентов. Анализ возможностей и объектов защиты с помощью ранее изученных уровневых сетевых моделей.

2. Система формирования режима информационной безопасности (1 час)

Система формирования режима информационной безопасности – многоуровневая система, обеспечивающая комплексную защиту информационных систем от вредных воздействий, наносящих ущерб субъектам информационных отношений. Законодательно-правовой уровень, административный уровень, программно-технический уровень.

3. **Нормативно-правовые основы информационной безопасности в РФ. (1 час)**

Нормативно-правовые основы информационной безопасности в РФ – законодательные меры в сфере информационной безопасности, направлены на создание в стране законодательной базы, упорядочивающей и регламентирующей поведение субъектов и объектов информационных отношений, а также определяющей ответственность за нарушение установленных норм.

4. **Стандарты информационной безопасности в РФ.(1 час)**

Стандарт ISO/IEC 15408 "Критерии оценки безопасности информационных технологий", требования безопасности к информационным системам, принцип иерархии: класс – семейство – компонент – элемент, функциональные требования, требования доверия.

5. **Оборудование сетей и представление об уязвимости аппаратного уровня** (1 час).

Типы аппаратуры в сетях Ethernet (коммуникаторы и повторители). Перехват информации. Методы защиты (коммутация, виртуальные локальные сети, шифрование), основы настройки аппаратуры, способы контроля (программы-сниферы). Демонстрация работы программ этого типа в школьной локальной сети.

6. **Уязвимости и атаки сетевого и транспортного уровней. Уязвимости и атаки прикладного уровня** (1 час).

Средства защиты: персональные брандмауэры, средства обнаружения атак. Создание правил, описание диапазонов адресов, контроль сетевой активности локальных приложений. Некоторые типы атак. Использование персональных брандмауэров для оптимизации работы в сети Интернет (в ранее изученных ситуациях).

Правила создания и замены паролей, разграничение доступа на основе пользовательских записей. Системы обновления ПО. Антивирусные программы, программы детектирования и удаления нежелательных внедрений. Проведение обновления ранее изученных программных комплексов.

7. **Тест. Обобщение пройденного материала по курсу «Информационная безопасность»** (1 час).

Итого: 7 часов

НЕОБХОДИМОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

1. Операционная система Windows 2000 или XP с разделом NTFS на жестком диске.
2. Персональный брандмауэр Agnitum Outpost (или аналогичный).
3. Антивирусный комплекс с доступом к системе обновлений (желательно - DrWeb).
4. Система выявления и удаления нежелательных программ AdAware Personal Edition (или аналогичная).
5. Стандартные средства для работы с сетью Интернет.
6. Серверный комплекс (при отсутствии связи с Интернет; для моделирования работы в сети).
7. Сканер уязвимостей XSpider Demo (или аналогичный) – для демонстрации учителем поведения системы под атакой и для выявления допущенных ошибок в конфигурации системы (дополнительный компонент).

ТРЕБОВАНИЯ К УРОВНЮ ПОДГОТОВКИ УЧАЩИХСЯ ПО ОКОНЧАНИИ КУРСА

Учащиеся должны:

знать:

- назначение и области использования основных технических средств ИКТ и информационных ресурсов;
- базовые принципы организации и функционирования компьютерных сетей;
- основные понятия информационной безопасности;
- основные опасности и ошибки при работе в сетях, методы борьбы с ними;
- понятия вируса, «троянской» программы; средства удаленного управления, средства борьбы с ними;
- способы удостоверения и контроля аутентичности ходящей и исходящей информации, методы проверки ее источников;
- правовые основы области защиты информации, персональных данных.

уметь:

- оперировать информационными объектами, используя имеющие знания о возможностях информационных и коммуникационных технологий, том числе создавать структуры хранения данных;
- пользоваться справочными системами и другими источниками справочной информации;
- соблюдать права интеллектуальной собственности на информацию;
- устанавливать и настраивать программные средства защиты;
- разграничивать доступ к ресурсам локальной машины;
- своевременно обновлять программное обеспечение;
- контролировать источники информации по их заголовкам и сертификатам;
- использовать полученные знания и навыки для организации собственной безопасной работы сети.

Календарно-тематический план

по предпрофильному курсу

«Информационная безопасность»

№	Тема занятия	Количество часов	Дата
1	Базовые определения	1	
2	Система формирования режима информационной безопасности	1	
3	Нормативно-правовые основы информационной безопасности в РФ	1	
4	Стандарты информационной безопасности в РФ	1	
5	Оборудование сетей и представление об уязвимости аппаратного уровня	1	
6	Уязвимости и атаки сетевого и транспортного уровней. Уязвимости и атаки прикладного уровня	1	
7	Тест « Информационная безопасность» Обобщение пройденного материала по курсу «Информационная безопасность»	1	

Список используемой литературы.

1. Информатика. Программы для общеобразовательных учреждений. 2-11 классы: методическое пособие / составитель М.Н. Бородин. – М.: БИНОМ. Лаборатория знаний,2010г.
2. Программа элективного курса «Основы информационной безопасности при работе в телекоммуникационных сетях» И.А. Калинин, Н.И. Самылкина