МОУ Академический лицей г.Томска

Принято:
решением кафедры
физико-математических и
информационных дисциплин
протокол № 26 от «3» июня 2011г.
зав. кафедрой _____Макарова Т.В.

Утверждено:
научно-методическим советом
МОУ Академического лицея г.Томска
протокол № 55 от «8» августа 2011г.
председатель Совета:
_____Тоболкина И.Н.

приказ № 161-О от «14» июня 2011г.

Программа элективного курса
«Информационная безопасность»
для 10-х профильных классов

Учитель:
Калашникова С.А.

Томск - 2011г.

Пояснительная записка

Количество часов: 8
Образовательные области: математика и информатика
Профили: физико-математический и информационно-технологический
Возрастная группа: 10 класс

В связи с реформой в школьном образовании и переходом на профильное обучение в старших классах, важную роль стали играть элективные курсы по выбору. В соответствии с одобренной Минобразования «Концепцией профильного обучения на старшей ступени общего образования» дифференциация содержания обучения в старших классах осуществляется на основе различных сочетаний курсов трёх типов: базовых, профильных, элективных.

Целью элективных курсов является удовлетворение разнообразных образовательных потребностей учащихся, которые могут возникнуть при изучении базового или профильного курса. Таким образом, элективный курс становится необходимым звеном, для создания из ученика специалиста в наиболее интересной для него области.

Возникновение индустрии обработки информации привело к необходимости изучать проблемы защиты информации. Данный курс дает представление об основных видах угроз информационной безопасности и способах защиты и сокрытия информации.

Цели курса:

Обеспечить овладение обучающимися знаниями по теме «Шифрование данных» и раскрыть роль шифрования данных в современном мире. Также необходимо привить обучающимся навыки сознательного и рационального использования методов шифрования в своей учебной и профессиональной деятельности.

Задачи курса:

- сформировать навыки элементарного построения криптосистем;
- сформировать начальные знания в области компьютерной стеганографии;
- изучить основные способы шифрования и дешифрования текста;
- реализовать технические и эвристические способности учащихся в ходе проектирования и программирования различных криптографических и стеганографических задач;
- развить навык анализа выполненной работы;
- воспитать у учащихся усидчивость и внимание;
- рассмотреть применение полученных навыков в различных областях знаний;
- развить у учащихся логическое мышление;
- сформировать у учащихся чёткое понимание стойкости шифра;

Планируемые результаты:

обучающиеся должны знать:

- терминологию по данному элективному курсу;
- принципы и структуру построения реальных криптографических и стеганографических систем;

- требования к криптографическим и стеганографическим системам;
- виды криптографических и стеганографических систем;
- основные понятия криптографии и стеганографии;
- симметрические и асимметрические криптосистемы;
- основы современной стеганографии.

уметь:

- создавать математические модели простых криптографических и стеганографических систем;
- оценивать стойкость созданного шифра;
- шифровать и дешифровать различные тексты;
- вставлять текст в графическое изображение, методом наименьшего бита;
- применять терминологию шифрования данных;
- различать методы шифрования и пользоваться ими при изучении данного курса.

Способы оценивания уровня достижения учащихся

Уровень достижения учащихся осуществляется по результатам выполнения практических классных и домашних заданий. Общая аттестационная оценка – «зачтено»/«не зачтено». «Не зачтено» ставится, если учащийся не выполнил текущие задания и не справился с итоговой работой.

Межпредметные связи

Знания, полученные при изучении курса, могут быть использованы на уроках математики, например при изучении комбинаторики. На уроках информатики, например при создании программ использующих связи с внешними файлами, при алгоритмизации математической модели.

Знания и умения, приобретённые при изучении курса, могут служить фундаментом для дальнейшего создания объектно-ориентированных программ по защите данных.

Программа курса

Курс рассчитан на 8 учебных часов, занятия проводятся 1 раз в неделю.

Данный курс предполагает традиционные формы работы с учащимися: лекционные, практические занятия, семинары, домашнюю работу и итоговое тестирование. Все занятия проводятся в компьютерном классе.

Введение. Информационная безопасность (1 ч.)

Вводятся понятия «информационная безопасность», рассматриваются виды угроз информационной безопасности и меры по безопасности информационных систем.

Введение в криптологию (1 ч.)

Кодирование и декодирование информации. Шифрование и кодирование. Криптография, криптоанализ, ключ, правило Керкгоффса, криптостойкость шифра.

Виды шифров. Симметричные шифры (2ч.)

Виды шифров. Симметричные шифры. Шифры перестановки, замены. Шифр Цезаря. Шифр Виженера. Магические квадраты. Поворотная решетка. Практическая работа: составление алгоритма шифрования.

Ассиметричные шифры (с открытым ключом) (1ч.)

Современные алгоритмы шифрования. Шифры с открытым ключом. Алгоритм RSA. Алгоритм формирования ключей, алгоритм шифрования.

Хэширование и пароли (1ч.)

Пароли, проблема хранения. Хэш-код, хэширование. Коллизии. Цифровая подпись.

Стеганография (1ч.)

Стеганография. Методы стеганографии для различных видов информации. Цифровые водяные знаки.

Итоговая работа (1ч.)

Итоговое тестирование, выполнение заданий на зашифровку и расшифровку сообщений.

Рекомендуемая литература

1. Э.В.Танова «Введение в криптографию: как защитить свое письмо от любопытных.» М. БИНОМ. Лаборатория знаний, 2007г.

2. А.В. Бабаш, Г.П. Шанкин «Криптография» Москва, СОЛОН-Р, 2002 г.

3. В.Г. Грибунов, И.Н. Оков, И.В. Туринцев «Цифровая стеганография» Москва, СОЛОН-Пресс, 2002 г.

4. Брассар Дж. Современная криптология. Мир ПК. №3. 1997.

5. Кнут Д. Искусство программирования на ЭВМ. Т.2: Получисленные алгоритмы. М.: Мир. 1977.

6. Шеннон К. Работы по теории информации и кибернетике. - М.: ИЛ, 1963.

7. Ященко В. В. Основные понятия криптографии // Математическое просвещение. Сер. 3. №2. 1998. С. 53-70.