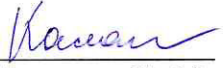


МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ АКАДЕМИЧЕСКИЙ ЛИЦЕЙ г. ТОМСКА
имени Г.А. ПСАХЬЕ

ПРИНЯТО:

Решением кафедры технологии и
точных наук МБОУ Академического
лицея г. Томска имени Г.А. Псахье
Зав. кафедрой

 Калашникова С.А.
Протокол № 66 от 25.05.2020 г.

УТВЕРЖДЕНО:

Научно-методическим Советом
МБОУ Академического лицея г.
Томска имени Г.А. Псахье
Председатель Совета, директор
О.В. Починок
Протокол № 107 от 28.08.2020 г.
Приказ № 299-О от 31.08.2020 г.



РАБОЧАЯ ПРОГРАММА ЭЛЕКТИВНОГО КУРСА

**«ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
И КРИПТОЛОГИИ»**

Уровень среднего общего образования
10 КЛАСС

Составитель
Калашникова Светлана
Аверьяновна

Пояснительная записка

Программа элективного курса «Основы информационной безопасности и криптологии» для 10 класса основана на учебно-методическом комплекте (далее УМК) Полякова К.Ю., Еремина Е.А., обеспечивающем обучение в соответствии с Федеральным государственным образовательным стандартом среднего (полного) общего образования (далее — ФГОС).

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:

Формировать установку на позитивную социальную деятельность в информационном обществе, на недопустимость действий, нарушающих правовые и этические нормы работы с информацией.

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 защиты информации в своей учебной и профессиональной деятельности.

Задачи курса:

- сформировать представление об основных способах защиты информации;
- 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;
- рассмотреть применение полученных навыков в различных областях знаний;
- сформировать у учащихся чёткое понимание стойкости шифра.

Особое внимание при изучении криптографии уделяется рассмотрению парадоксальных логических задач, так как все парадоксальное вызывает живой интерес учащихся, что создает мотивацию к изучению данного предмета. Кроме того, многие задачи имеют связь с реальной жизнью, что также повышает значимость рассматриваемых задач. Содержание учебной деятельности определяется системой учебных задач. Система задач будет удовлетворять требованиям системности и полноты, отражать межпредметные связи криптографии с другими учебными дисциплинами, обеспечивать формирование способов интеллектуальной и практической деятельности, а также использование компьютера не только, как инструмента решения задач, но и как средства получения знания и развития. Отбор содержания обучения

производился с учетом современной концепции обучения информатике, концепции профильного обучения.

Таким образом, изучение криптографии носит интегративный характер, так как в ней представлена естественная реализация межпредметных связей с другими дисциплинами. Реализация межпредметных связей позволяет увидеть одни и те же предметы, явления или процессы с разных точек зрения, получить целостное представление о мире, охватить все свойства и связи изучаемых объектов.

Место элективного курса в учебном плане: курс реализуется за счет вариативного компонента, формируемого участниками образовательного процесса. Общий объем курса – 8 часов, по 1 часу в неделю.

Формы проведения занятий: лекции, практические занятия, самостоятельная работа. Программой предусмотрены **методы обучения:** объяснительно-иллюстративные, эвристическая беседа, частично-поисковые, практические.

Способы оценивания уровня достижения учащихся

Контроль достижений учащихся осуществляется по результатам выполнения практических классных и домашних заданий, в том числе выполненных с применением дистанционных технологий. Для успешной аттестации по курсу обучающимся необходимо выполнить тест по теоретической части курса и итоговую работу по практической части.

1. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ КУРСА

Изучение криптографии способствует:

- интеллектуальному развитию учащихся;
- формированию межпредметных связей и развитию логического и абстрактного мышления путем решения нестандартных задач (задач, имеющих много вариантов решения или не имеющих алгоритма для решения);
- развитию дискретного математического мышления в процессе углубленного изучения криптографии через элементы теории графов;
- развитию способностей к анализу: выявлению взаимосвязей, вычленению существенного, нахождению закономерностей, классификации по общему признаку и т.п.;
- развитию способностей к концентрации внимания, к логическим рассуждениям, к созданию зрительных образов, умению принимать верные решения, ясно и творчески мыслить.

Выпускник научится:

- 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;
- соблюдать требования информационной безопасности, этики и права;
- искать и обрабатывать информацию из различных источников;
- интерпретировать изучаемые явления и процессы, давать им сущностные характеристики;
- 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.

Выпускник получит возможность научиться:

- различать основные виды информационно-психологических воздействий в виртуальной реальности;
- высказывать критическую точку зрения и свои суждения по проблемным вопросам;
- приводить собственные примеры явлений и тенденций, связанных с безопасностью информационного общества.

2. СОДЕРЖАНИЕ ПРОГРАММЫ

Введение. Информационная безопасность.

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

Введение в криптологию.

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

Виды шифров. Симметричные шифры.

Виды шифров. Симметричные шифры. Шифры перестановки, замены. Шифр Цезаря. Шифр Виженера. Магические квадраты. Поворотная решетка.

Ассиметричные шифры (с открытым ключом).

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

Хэширование и пароли.

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

Стеганография.

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

Итоговая работа.

3. ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ

№	Тема	Кол-во часов
1	Введение. Информационная безопасность	1
2	Введение в криптологию	1
3	Виды шифров. Симметричные шифры.	1
4	Ассиметричные шифры (с открытым ключом)	1
5	Практическая работа	1
6	Хэширование и пароли	1
7	Стеганография	1
8	Итоговая работа	1
	Всего	8

Информационно-методическое обеспечение

1. Поляков К. Ю. Информатика. 10 класс. Базовый и углубленный уровни : учебник : в 2 ч. Ч. 1 / К. Ю. Поляков, Е. А. Еремин. — М. : БИНОМ. Лаборатория знаний, 2019.
2. <https://вбезопасныйинтернет.рф/lessons-video>
3. <http://www.i-deti.org/>