Министерство образования и науки Астраханской области
государственное автономное образовательное учреждение
Астраханской области дополнительного образования
«Региональный школьный технопарк»
отдел «Технопарк»

ПРИНЯТО:
Решением Педагогического
совета ГАОУ АО ДО «РШТ»
от «12» марта 2020 г.
Протокол № 05

УТВЕРЖДАЮ:
Директор ГАОУ АО ДО «РШТ»
_____ Войков В.В.
«12» марта 2020 г.

Дополнительная общеобразовательная общеразвивающая программа математической направленности «Расширенный курс криптографии» (с применением дистанционных технологий)

Возрастная категория: 5-11 класс
Срок реализации: 55 академических часа

Составитель:
Лим В.Г.
преподаватель

Астрахань, 2020 г.

Оглавление

Пояснительная записка

Дополнительная общеразвивающая программа «Расширенный курс криптографии» имеет математическую направленность.

Уровень программы – базовый.

Актуальность программы

Дополнительная общеразвивающая программа «Расширенный курс криптографии» относится к направлению «Математика» базового уровня обучения.

Криптография (от греч. κρυπτός — скрытый и γράφω — писать) – древнейшая наука о способах защиты конфиденциальных данных от нежелательного стороннего прочтения. Криптоанализ – наука, изучающая методы нарушения конфиденциальности информации. Криптанализ и криптография вместе составляют науку криптологию, изучающую способы шифрования и дешифрования..

Средства криптографической защиты гостайны до сих пор приравниваются к оружию. Очень немногие страны мира имеют свои криптографические компании, которые делают действительно хорошие средства защиты информации. Даже во многих развитых странах нет такой возможности: там отсутствует школа, которая позволяла бы эти технологии поддерживать и развивать. Россия одна из немногих стран мира, – может быть таких стран пять, или около того, – где все это развито. Причем и в коммерческом, и в государственном секторе есть компании и организации, которые сохранили преемственность школы криптографии с тех времен, когда она только зарождалась.

В настоящее время действия злоумышленников являются основным источников угроз применению информационных технологий в современном обществе, и, в частности, в сфере образования. В связи с этим становится актуальной задача обучения школьников и студентов основам компьютерной безопасности.

Достигнутые в последние годы успехи в развитии прикладных научных исследований неотделимы от достижений в обработке данных с использованием современных информационных технологий. Очевидно, что необходимо внедрять в практику обучение современным методам обработки информации, что требует совершенствования образовательных технологий. В настоящее время в школьную программу включен предмет «Информатика», в образовательных учреждениях дополнительного образования в течение ряда лет ведется обучение программированию, 3D-моделированию, технологиям построения вычислительных сетей и т.д. При этом участие в занятиях принимают ученики 5-6 и даже 3-4 класса. Практика свидетельствует о положительных результатах обучения.

В нашей стране создана современная система обучения в области информационной безопасности. Организационно-методическую основу данной системы обеспечивает Учебно-методическое объединение (УМО) вузов России по образованию в сфере информационной безопасности на базе института криптографии, связи и информатики (ИКСИ) Академии ФСБ России. В течение

двадцати с лишним лет в России ежегодно проводится Межрегиональная олимпиада по криптографии и математике, в которой принимают участие ученики 9-11 классов общеобразовательных школ из всех регионов Российской Федерации. Так как информационная безопасность и криптография не входят в школьную программу, во многих вузах России организованы кружки по криптографии, одной из главных задач которых является подготовка школьников к участию в межрегиональной олимпиаде по криптографии.

Региональный школьный технопарк с 2016 года проводит занятия с учащимися общеобразовательных школ по основам информационной безопасности и криптографии. Занятия развивают интеллектуальные способности школьников и положительно влияют на их успеваемость в общеобразовательной школе. Дети в раннем возрасте начинают понимать, в каком направлении может в будущем развиваться их профессиональная деятельность.

Программа разработана и реализуется на основе следующих нормативно - правовых документов:

- Федеральный закон от 29.12.2012г. № 273-ФЗ «Об образовании в Российской Федерации»;
- Постановление от 4 июля 2014г. №42 «Об утверждении СанПиН 2.4.4.3172-14 «Санитарно-эпидемиологические требования к устройству, содержанию и организации режима работы образовательных организаций дополнительного образования детей»;
- Письмо Министерства образования и науки РФ от 18 ноября 2015г. № 09-3242 «Методические рекомендации по проектированию дополнительных общеразвивающих программ»;
- Приказ Министерства образования и науки РФ от 29 августа 2013г. № 1008 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным общеобразовательным программам»;
- Распоряжение Правительства Российской Федерации от 04 сентября 2014г. № 1726р «Об утверждении Концепции развития дополнительного образования детей»;
- Государственная программа Российской Федерации «Развитие образования» на 2013-2020 годы;
- Стратегия развития воспитания в РФ до 2025года.

Целью данной программы является получение обучающимися базовых знаний в области информационной безопасности и криптографии.

Для реализации этой цели необходимо решить следующие задачи:

- изучить основные способы шифрования, расшифрования и дешифрования текста;
- реализовать эвристические способности учащихся в ходе решения различных криптографических задач;
- развить у учащихся навыки логического мышления;
- развить у учащихся навыки анализа выполненной работы, рассмотреть применение полученных навыков в различных областях знаний;

• воспитать у учащихся усидчивость и внимание;

• подготовить к дальнейшему обучению по направлению в высших учебных заведениях.

Учащиеся, для которых программа актуальна

Возраст обучающихся по данной программе: 5 – 11 класс.

Количество обучающихся в группе: 6 – 10 человек.

При составлении программы были учтены возрастные, психолого-педагогические, физические особенности детей.

Дети младшего возраста (от 11 лет), обладают достаточно хорошей фантазией, что помогает им придумывать довольно изобретательные способы решения проблем.

Формы и режим занятий

Форма занятий – очная (дистанционная).

Занятия проходят 1 или 2 раза в неделю по 3 академических часа, с перерывом 10 минут.

Срок реализации программы

Срок реализации программы – 73 академических часа.

Планируемые результаты

В результате обучения, учащиеся будут

знать:

• основные типы шифров;

• основы применения шифров для решения задач защищенного обмена информацией;

• математические основы криптографии;

• основы криптоанализа;

• базовые принципы построения шифров;

• базовые принципы криптографической защиты информации.

• **уметь:**

• применять основные методы шифрования и расшифрования информации;

• находить решения типовых криптографических задач;

• применять основные методы криптоанализа для дешифрования закрытых текстов.

Формы и средства контроля.

Формы контроля

Реализация программы «Расширенный курс криптографии» предусматривает входной и итоговый контроль освоения обучающимися программы.

Входной контроль необходим при приеме учащихся на программу базового уровня «Расширенный курс криптографии». Приём обучающихся на курс по программе «Расширенный курс криптографии» производится по результатам освоения программы вводного уровня «Основы криптографии», либо по результатам, достигнутым школьниками в областных и

межрегиональных олимпиадах по математике и криптографии. Для зачисления в группу, обучение в которой будет проводиться по программе «Расширенный курс криптографии», школьнику необходимо обучение по дополнительной общеобразовательной общеразвивающей программе «Основы криптографии», или принять участие в областной или межрегиональной Олимпиаде школьников, при этом требуется решить правильно не менее одной задачи в межрегиональной олимпиаде или не менее двух задач в областной Олимпиаде школьников по математике и криптографии в текущем году или году, предшествующем приему учащегося на обучение по программе базового уровня «Расширенный курс криптографии».

Итоговый контроль проводится с целью определения уровня усвоения обучающимися программного материала в целом.

Итоговый контроль осуществляется в форме публичного выступления в виде защиты проекта посредством демонстрации презентации и научного доклада на научно-технической конференции Schooltech Conference.

Средства контроля

Средства контроля уровня освоения обучающимися пройденного материала в данной программе являются:

- педагогическое наблюдение;
- опрос;
- выступление в виде защиты проекта посредством презентации на научно – технической конференции Schooltech Conference.

Учебно-тематический план

№ п/п	Название темы/раздела	Количество часов			Формы аттестации/ контроля
		Всего	Теория	Практика	
1	**Раздел 1. Введение в криптологию**	**10**	**4**	**6**	**Педагогическое наблюдение Опрос**
1.1	История криптографии и исторические шифры	4	2	2	
1.2	Введение в криптологию и основные термины	2	2		
1.3	Решение практических задач	4		4	
2	**Раздел 2. Моноалфавитные шифры замены**	**15**	**8**	**7**	**Педагогическое наблюдение Опрос**
2.1	Система аддитивных (или сдвиговых) шифров.	1	1		
2.2	Введение в модульную арифметику	2	2		
2.3	Методы криптоанализа аддитивных шифров	2	1	1	
2.4	Мультипликативные	1	1		

№ п/п	Название темы/раздела	Количество часов			Формы аттестации/ контроля
		Всего	Теория	Практика	
	шифры замены				
2.5	Методы криптоанализа мультипликативных шифров	2	1	1	
2.6	Решение практических задач	2		2	
2.7	Аффинный шифры замены	1	1		
2.8	Методы криптоанализа аффинных шифров	2	1	1	
2.9	Разбор Олимпиадных задач	2		2	
3	**Раздел 3. Полиалфавитные шифры замены**	**12**	**5**	**7**	**Педагогическое наблюдение Опрос**
3.1	Шифры полиалфавитной замены, шифр Гронсфелда	1	1		
3.2	Шифры гаммирования, типы шифрующих последовательностей и их применение	1	1		
3.3	Шифр Виженера. Выбор между моноалфавитным и полиалфавитным шифрами.	2	1	1	
3.4	Решение практических задач	2		2	
3.5	Методы криптоанализа шифра Виженера	1	1		
3.6	Метод индекса совпадений. Вскрытие шифра Виженера	2	1	1	
3.7	Разбор Олимпиадных задач	3		3	
4	**Раздел 4. Асимметричные системы шифрования. Практические основы современной криптографии**	**12**	**6**	**6**	**Педагогическое наблюдение Опрос**
4.1	Симмстричные и асимметричные криптографические	2	2		

№ п/п	Название темы/раздела	Количество часов			Формы аттестации/ контроля
		Всего	Теория	Практика	
	системы. Методы распределения ключей в системах шифрования				
4.2	Двухключевые криптографические системы (с открытым ключом). Применение шифрования с открытым ключом.	2	2		
4.3	Решение практических задач	3		3	
4.4	Понятие односторонних функций. Шифрование RSA. Шифрование Эль-Гамаля	2	2		
4.5	Разбор Олимпиадных задач	3		3	
5	**Раздел 5. Подготовка к публичному выступлению в виде защиты проекта посредством презентации на научно – технической конференции Schooltech Conference.**	**6**		**6**	**Публичное выступление в виде защиты проекта посредством презентации на научно – технической конференции Schooltech Conference.**
5.1	Уточнение темы итогового проекта	2		2	
5.2	Подготовка презентации	2		2	
5.3	Подготовка научного доклада	2		2	
	Всего	**55**	**23**	**32**	

Содержание учебно-тематического плана

Тема	Вид учебного занятия, учебных работ	Оборудование, материалы	Содержание
1.1. История криптографии и исторические шифры	Лекция и практические занятия	Компьютер (ноутбук) с доступом к сети интернет видеокамерой и гарнитурой, интерактивная панель или проектор, кабель HDMI, маркерная доска, маркеры (чёрный, красный, синий и зелёный)	**Теория:** Введение в историю криптографию и рассмотрение наиболее известных исторических шифров **Практика:** Рассмотрение практических примеров применения шифров
1.2 Введение в криптологию и основные термины	Лекция	Компьютер (ноутбук) с доступом к сети интернет видеокамерой и гарнитурой, интерактивная панель или проектор, кабель HDMI, маркерная доска, маркеры (чёрный, красный, синий и зелёный)	**Теория:** Основные понятия криптологии: шифр, ключ, шифрование, расшифрование, дешифрование, криптоанализ, методы криптоанализа, вскрытие шифров
1.3. Решение практических задач	Практические занятия	Компьютер (ноутбук) с доступом к сети интернет видеокамерой и гарнитурой, интерактивная панель или проектор, кабель HDMI, маркерная доска, маркеры (чёрный, красный, синий и зелёный)	**Практика:** Знакомство с методами криптоанализа, изучение стойкости криптосистем
2.1. Система аддитивных (или сдвиговых) шифров.	Лекция	Компьютер (ноутбук) с доступом к сети интернет видеокамерой и гарнитурой, интерактивная панель или проектор, кабель HDMI, маркерная доска, маркеры (чёрный, красный, синий и	**Теория:** Знакомство с моноалфавитными шифрами замены, примеры шифров, шифр Цезаря, система аддитивных (или сдвиговых) шифров. Основы модульной арифметики. Решение

Тема	Вид учебного занятия, учебных работ	Оборудование, материалы	Содержание
		зелёный)	практических задач
2.2. Введение в модульную арифметику	Лекция	Компьютер (ноутбук) с доступом к сети интернет видеокамерой и гарнитурой, интерактивная панель или проектор, кабель HDMI, маркерная доска, маркеры (чёрный, красный, синий и зелёный)	**Теория:** Изучение основ модульной арифметики. Модуль системы, остатки от деления, арифметика остатков, понятие аддитивной инверсии
2.3 Методы криптоанализа аддитивных шифров	Лекция и практические занятия	Компьютер (ноутбук) с доступом к сети интернет видеокамерой и гарнитурой, интерактивная панель или проектор, кабель HDMI, маркерная доска, маркеры (чёрный, красный, синий и зелёный)	**Теория:** Рассмотрение методов криптоанализа аддитивных шифров: полный перебор, частотный анализ **Практика:** Рассмотрение примеров задач областных олимпиад по криптографии
2.4 Мультипликативные шифры замены	Лекция	Компьютер (ноутбук) с доступом к сети интернет видеокамерой и гарнитурой, интерактивная панель или проектор, кабель HDMI, маркерная доска, маркеры (чёрный, красный, синий и зелёный)	**Теория:** Мультипликативный шифр, Ограничения на мультипликативные ключи. Понятие и Определение мультипликативной инверсии.
2.5 Методы криптоанализа мультипликативных шифров	Лекция и практические занятия	Компьютер (ноутбук) с доступом к сети интернет видеокамерой и гарнитурой, интерактивная панель или проектор, кабель HDMI, маркерная доска, маркеры (чёрный, красный, синий и зелёный)	**Теория:** Рассмотрение методов криптоанализа мультипликативных шифров: перебор ключей и частотный анализ. **Практика:** Вскрытие мультипликативного шифра. Решение практических задач

Тема	Вид учебного занятия, учебных работ	Оборудование, материалы	Содержание
2.6 Решение практических задач	Практические занятия	Компьютер (ноутбук) с доступом к сети интернет видеокамерой и гарнитурой, интерактивная панель или проектор, кабель HDMI, маркерная доска, маркеры (чёрный, красный, синий и зелёный)	**Практика:** Знакомство с криптоанализом моноалфавитных шифров, практические примеры применения и типовые задачи
2.7 Аффинный шифры замены	Лекция	Компьютер (ноутбук) с доступом к сети интернет видеокамерой и гарнитурой, интерактивная панель или проектор, кабель HDMI, маркерная доска, маркеры (чёрный, красный, синий и зелёный)	**Теория:** Знакомство с принципами аффинного шифрования. Схема аффинного шифрования, требования к аддитивному и мультипликативному ключам, вычисление обратных ключей.
2.8 Методы криптоанализа аффинных шифров	Лекция и практические занятия	Компьютер (ноутбук) с доступом к сети интернет видеокамерой и гарнитурой, интерактивная панель или проектор, кабель HDMI, маркерная доска, маркеры (чёрный, красный, синий и зелёный)	**Теория:** Рассмотрение методов криптоанализа аффинных шифров. Вскрытие аффинного шифра и частотный анализ. Практика: Примеры вскрытия аффинного шифра. Решение практических задач
2.9 Разбор Олимпиадных задач	Практические занятия		**Практика:** Знакомство с криптоанализом моноалфавитных шифров, рассмотрение примеров Олимпиадных задач
3.1. Шифры полиалфавитной замены, шифр Гронсфелда	Лекция	Компьютер (ноутбук) с доступом к сети интернет видеокамерой и гарнитурой,	**Теория:** Шифры полиалфавитной замены, преимущества полиалфавитных

Тема	Вид учебного занятия, учебных работ	Оборудование, материалы	Содержание
		интерактивная панель или проектор, кабель HDMI, маркерная доска, маркеры (чёрный, красный, синий и зелёный)	шифров, шифр Гронсфелда
3.2. Шифры гаммирования, типы шифрующих последовательностей и их применение	Лекция	Компьютер (ноутбук) с доступом к сети интернет видеокамерой и гарнитурой, интерактивная панель или проектор, кабель HDMI, маркерная доска, маркеры (чёрный, красный, синий и зелёный)	**Теория:** Шифры гаммирования. Теоретические основы и практическое применение. Типы шифрующих последовательностей. Примеры шифрующих последовательностей
3.3 Шифр Виженера. Выбор между моноалфавитным и полиалфавитным шифрами.	Лекция и практические занятия	Компьютер (ноутбук) с доступом к сети интернет видеокамерой и гарнитурой, интерактивная панель или проектор, кабель HDMI, маркерная доска, маркеры (чёрный, красный, синий и зелёный)	**Теория:** Особенности и преимущества полиалфавитных шифров. Шифрование методом Виженера. **Практика:** Решение практических задач. Рассмотрение примеров задач
3.4 Решение практических задач	Практические занятия	Компьютер (ноутбук) с доступом к сети интернет видеокамерой и гарнитурой, интерактивная панель или проектор, кабель HDMI, маркерная доска, маркеры (чёрный, красный, синий и зелёный)	**Практика:** Знакомство с криптоанализом полиалфавитных шифров, практические примеры применения и типовые задачи
3.5 Методы криптоанализа шифра Виженера	Лекция	Компьютер (ноутбук) с доступом к сети интернет видеокамерой и гарнитурой, интерактивная	**Теория:** Методы криптоанализа полиалфавитных шифров, тест Касиски, применение теста Касиски для

Тема	Вид учебного занятия, учебных работ	Оборудование, материалы	Содержание
		панель или проектор, кабель HDMI, маркерная доска, маркеры (чёрный, красный, синий и зелёный)	вскрытия шифра Виженера. Выбор между моноалфавитным и полиалфавитным шифрами, тест Фридмана.
3.6 Метод индекса совпадений. Вскрытие шифра Виженера	Лекция и практические занятия	Компьютер (ноутбук) с доступом к сети интернет видеокамерой и гарнитурой, интерактивная панель или проектор, кабель HDMI, маркерная доска, маркеры (чёрный, красный, синий и зелёный)	**Теория:** Применение метода индекса совпадений для вскрытия шифра Виженера **Практика:** Рассмотрение практических примеров вскрытия шифра Виженера
3.7. Разбор Олимпиадных задач	Практические занятия	Компьютер (ноутбук) с доступом к сети интернет видеокамерой и гарнитурой, интерактивная панель или проектор, кабель HDMI, маркерная доска, маркеры (чёрный, красный, синий и зелёный)	**Практика:** Знакомство с полиалфавитными шифрами, примеры шифров, методы вскрытия шифров, разбор задач межрегиональной Олимпиады школьников по математике и криптографии
4.1. Симметричные и асимметричные криптографические системы. Методы распределения ключей в системах шифрования	Лекция	Компьютер (ноутбук) с доступом к сети интернет видеокамерой и гарнитурой, интерактивная панель или проектор, кабель HDMI, маркерная доска, маркеры (чёрный, красный, синий и зелёный)	**Теория:** Понятие криптосистемы. Сравнение симметричных и асимметричных криптосистем. Методы распределения ключей в симметричных и асимметричных криптосистемах
4.2 Двухключевые криптографические системы (с открытым ключом). Применение шифрования с	Лекция	Компьютер (ноутбук) с доступом к сети интернет видеокамерой и гарнитурой, интерактивная	**Теория:** Двухключевые криптографические системы (с открытым ключом).

Тема	Вид учебного занятия, учебных работ	Оборудование, материалы	Содержание
открытым ключом		панель или проектор, кабель HDMI, маркерная доска, маркеры (чёрный, красный, синий и зелёный)	Применение шифрования с открытым ключом. Схема шифрования с открытым ключом.
4.3. Решение практических задач	Практические занятия	Компьютер (ноутбук) с доступом к сети интернет видеокамерой и гарнитурой, интерактивная панель или проектор, кабель HDMI, маркерная доска, маркеры (чёрный, красный, синий и зелёный)	**Практика:** Знакомство с шифрованием с открытым ключом, разбор типовых задач
4.4. Понятие односторонних функций. Шифрование RSA. Шифрование Эль-Гамаля	Лекция	Компьютер (ноутбук) с доступом к сети интернет видеокамерой и гарнитурой, интерактивная панель или проектор, кабель HDMI, маркерная доска, маркеры (чёрный, красный, синий и зелёный)	**Теория:** Понятие односторонней функции. Шифры, основанные на решении задачи факторизации целых чисел. Шифры, основанные на решении задачи дискретного логарифмирования. Шифр RSA. Шифр Эль-Гамаля.
4.5. Разбор Олимпиадных задач	Практические занятия	Компьютер (ноутбук) с доступом к сети интернет видеокамерой и гарнитурой, интерактивная панель или проектор, кабель HDMI, маркерная доска, маркеры (чёрный, красный, синий и зелёный)	**Практика:** Практическое знакомство с шифрованием RSA и односторонними функциями. Разбор олимпиадных задач.
5.1. Уточнение темы итогового проекта	Практические занятия	Компьютер (ноутбук) с доступом к сети интернет видеокамерой и гарнитурой, интерактивная	**Практика:** Рассмотрение аналогов, обсуждение темы проекта, выбор темы проекта

Тема	Вид учебного занятия, учебных работ	Оборудование, материалы	Содержание
		панель или проектор, кабель HDMI, маркерная доска, маркеры (чёрный, красный, синий и зелёный)	
5.2. Подготовка презентации	Практические занятия	Компьютер (ноутбук) с доступом к сети интернет видеокамерой и гарнитурой, интерактивная панель или проектор, кабель HDMI, маркерная доска, маркеры (чёрный, красный, синий и зелёный)	**Практика:** Подготовка презентации обучающимися. Корректировка презентации преподавателем.
5.3. Подготовка научного доклада	Практические занятия	Компьютер (ноутбук) с доступом к сети интернет видеокамерой и гарнитурой, интерактивная панель или проектор, кабель HDMI, маркерная доска, маркеры (чёрный, красный, синий и зелёный)	**Практика:** Подготовка научного доклада, обсуждение итогового проекта, подготовка к итоговому выступлению на научно – технической конференции Schooltech Conference.
5.4 Защита проекта	Практические занятия	Компьютер (ноутбук) с доступом к сети интернет видеокамерой и гарнитурой, интерактивная панель или проектор, кабель HDMI, маркерная доска, маркеры (чёрный, красный, синий и зелёный)	**Практика:** Итоговое выступление с научным докладом на научно-технической конференции Schooltech Conference.

Организационно-педагогические условия реализации программы

Материально-технические условия реализации программы

Требования к помещению для занятий:

Для комфортной работы обучающихся необходимо достаточно освещенное, просторное помещение. Также необходимы стулья (10-15 стульев).

Для чтения лекций необходимы маркерная или интерактивная доска и компьютер с проектором и экраном для демонстрации слайдов.

Для решения задач необходима маркерная доска.

Для подготовки демонстрационных материалов необходимы компьютер а также цветной лазерный принтер.

Для комфортной работы обучающихся с применением дистанционных технологий необходим компьютер или другое электронное устройство с доступом к сети Интернет.

Расходные материалы:

Для осуществления проектной деятельности необходимо иметь следующие инструменты и материалы:

- маркеры разных цветов;
- картриджи для лазерной печати;
- бумага для печати материалов;

Список литературы

Нормативно-правовые акты и документы:

1 Концепция развития дополнительного образования детей (утверждена распоряжением Правительства Российской Федерации от 04 сентября 2014 г. № 1726-р).

2 Методические рекомендации по проектированию дополнительных общеразвивающих программ (включая разноуровневые программы): приложение к письму Министерства образования и науки Российской Федерации от 18 ноября 2015 г. № 09-3242.

3 Приказ Министерства просвещения РФ от 9 ноября 2018г. №196 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным общеобразовательным программам».

4 СанПиН 2.4.4.3172-14 «Санитарно-эпидемиологические требования к устройству, содержанию и организации режима работы образовательных организаций дополнительного образования детей» (утверждены постановлением Главного государственного санитарного врача Российской Федерации от 4 июля 2014 г. № 41).

5 Федеральный закон от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации».

Литература для педагогов:

1. Лим, В.Г., Кабулов Б.Т. Практические основы криптографии / В.Г. Лим, Б.Т. Кабулов. - Астрахань: Издатель: Сорокин Роман Васильевич, 2019. - 310 с.

2. Адаменко, М. Основы классической криптологии. Секреты шифров и кодов / Михаил Адаменко. - Москва: ДМК-Пресс, 2016. - 296 с.

3. Бабаш, А.В. История криптографии. Часть 1 / А.В. Бабаш, Г.П. Шапкин. - М.: Гелиос АРВ, 2002. - 240 с.

4. Бабенко, Л.К. Криптографическая защита информации: симметричное шифрование: учебное пособие для вузов / Л.К. Бабенко, Е.А. Ищукова. – М.: Издательство Юрайт, 2017. – 220 с. – Серия: Университеты России.

5. Баричев, С.Г. Основы современной криптографии / С.Г. Баричев, В.В. Гончаров, Р.Е. Серов. - Москва: СИНТЕГ, 2011. - 176 с.

6. Бутырский, Л.С. Криптографический фронт Великой Отечественной / Бутырский Л.С., Ларин Д.А., Шапкин Г.П. – М.: Гелиос АРВ, 2017. – 688 с.

7. Герман, О.Н. Теоретико-числовые методы в криптографии / О.Н. Герман, Ю.В. Нестеренко. - М.: Академия, 2012. - 272 с.

8. Здор, С.Е. Кодирующая информация. От первых природных кодов до искусственного интеллекта / С.Е. Здор. - М.: Либроком, 2012. - 168 с.

9. Земор, Ж. Курс криптографии / Ж. Земор. - М.: Регулярная и хаотическая динамика, Институт компьютерных исследований, 2006. - 256 с.

10. Зубов, А.Ю. Олимпиады по криптографии и математике для школьников / А.Ю. Зубов, А.В. Зязин, Н.В. Никонов, С.М. Рамоданов, А.С. Фролов.– 2-е изд. перераб. и доп. – М.: МЦНМО, 2013. – 154 с.

11. Информационный мир XXI века. Криптография – основа информационной безопасности / Под. ред. Э.А. Болелова; Московский государственный технический университет гражданской авиации. – М.: Издательско-торговая корпорация «Дашков и К°», 2017. – 126 с.

12. Коблиц, Н. Курс теории чисел и криптографии / Н. Коблиц. – М.: Научное издательство ТВП, 2001.

13. Лось, А.Б. Криптографические методы защиты информации: учебник для академического бакалавриата / А.Б. Лось, А.Ю. Нестеренко, М.И. Рожков. – 2-е изд., испр. – М.: Издательство Юрайт, 2016. – 473 с. – Серия: Бакалавр. Академический курс.

14. Митани Масааки, Сато Синъити, Криптография. Манга / Митани Масааки, Сато Синъити (авторы), Хиноки Идеро (художн.); пер. с яп. Клюпского А.Б., научн. ред. Л.М. Белявский. – М.: ДМК Пресс, 2019. – 238 с.

15. Паропин, А.А. Информационная безопасность: стандартизированные термины и понятия. / А.А. Паропин. - Владивосток: Изд-во Дальневост. Ун-та, 2010. - 216 с.

16. Полянская, О.Ю. Инфраструктуры открытых ключей. Учебное пособие / О.Ю. Полянская, В.С. Горбатов. - М.: Интернет-университет информационных технологий; Бином. Лаборатория знаний, 2007. – 368 с.

17. Смарт, Н. Криптография / Н. Смарт. – М.: Техносфера, 2005.

18. Столлинг, В. Криптография и защита сетей: принципы и практика, 2-е изд. / В. Столлинг. – М.: Издательский дом «Вильямс», 2001, - 672 с.

19. Тайные знаки / Под ред. Пола Литле. – М.: ООО «Издательство «Вокруг Света», 2011. – 290 с.

20. Фергюсон, Шнье, Шнайер, Брюс. Практическая криптография / Брюс Шнайер, Шнье Фергюсон. – М.: Издательский дом «Вильяме», 2005. – 424 с.

21. Фомичёв, В.М. Криптографические методы защиты информации. В 2 ч. Часть 1. Математические аспекты: учебник для академического бакалавриата / В.М. Фомичёв, Д.А. Мельников; под. ред. В.М. Фомичева. – М.: Издательство Юрайт, 2016. – 209 с. – Серия: Бакалавр. Академический курс.

22. Фомичёв, В.М. Криптографические методы защиты информации. В 2 ч. Часть 2. Системные и прикладные аспекты: учебник для академического бакалавриата / В.М. Фомичёв, Д.А. Мельников; под. ред. В.М. Фомичева. – М.: Издательство Юрайт, 2016. – 245 с. – Серия: Бакалавр. Академический курс.

23. Ховард, М. 24 смертных греха компьютерной безопасности / М. Ховард, Д. Лебланк, Дж. Вьега. - М.: Питер, 2010. - 400 с.

24. Черемушкин, А.В. Лекции по арифметическим алгоритмам в криптографии / А.В. Черемушкин. - М.: МЦНМО, 2002. - 104 с.

25. Черчхаус, Роберт. Коды и шифры. Юлий Цезарь, «Энигма» и Интернет / Роберт Черчхаус. – М.: Издательство «Весь Мир», 2005. - 308 с.

26. Шнайер, Брюс. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си: моногр. / Брюс Шнайер. - М.: Триумф, 2012. - 816 с.

27. Шумский, А.А. Системный анализ в защите информации / А.А. Шумский. - Москва: СПб. [и др.]: Питер, 2005. - 224 с.

28. Ященко, В.В. Введение в криптографию / Под. общ. ред. В.В. Ященко. -М.: МЦНМО, 2012. – 348 с.

29. Dooley F. John. History of Cryptography and Cryptanalysis. Codes, Ciphers, and Their Algorithms / John F. Dooley, Springer International Publishing AG, part of Springer Nature 2018. Library of Congress Control Number: 2018942943, 308 p.

30. Klima Richard, Sigmon Neil. Cryptology. Classical and Modern. Second Edition / Richard Klima, Neil Sigmon, CRC Press, 2019, 498 p.

31. Schwartz Stu. Cryptology for Beginners / Stu. Schwartz, Ambler, Palo Alto, 19002, 62 p.

Литература для детей:

1. Лим, В.Г., Кабулов Б.Т. Практические основы криптографии / В.Г. Лим, Б.Т. Кабулов. - Астрахань: Издатель: Сорокин Роман Васильевич, 2019. - 310 с.

2. Зубов, А.Ю. Олимпиады по криптографии и математике для школьников / А.Ю. Зубов, А.В. Зязин, П.В. Пикопов, С.М. Рамоданов, А.С. Фролов.– 2-е изд. перераб. и доп.– М.: МЦНМО, 2013. – 154 с.

3. Информационный мир XXI века. Криптография – основа информационной безопасности / Под. ред. О.А. Болелова; Московский государственный технический университет гражданской авиации. – М.: Издательско-торговая корпорация «Дашков и К°», 2017. – 126 с.

4. Миташи Масааки, Сато Синъити. Криптография. Манга / Миташи Масааки, Сато Синъити (авторы), Хиноки Идеро (художн.); пер. с яп. Клюпского А.Б., научн. ред. Д.М. Белявский. – М.: ДМК Пресс, 2019. – 238 с.

5. Ященко, В.В. Введение в криптографию / Под. общ. ред. В.В. Ященко. - М.: МЦНМО, 2012. – 348 с.