ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ДОПОЛНИТЕЛЬНОГО ОБРАЗОВАНИЯ
«ЦЕНТР ДЛЯ ОДАРЕННЫХ ДЕТЕЙ «ПОИСК»

РЕКОМЕНДОВАНА

педагогическим советом
Протокол от «24» августа 2020

УТВЕРЖДАЮ

Заведующая филиалом
_____ Т.В.Ларина

ДОПОЛНИТЕЛЬНАЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ОБЩЕРАЗВИВАЮЩАЯ КОММЕРЧЕСКАЯ ПРОГРАММА

«Шифрование данных»

Возраст обучающихся: 13-17 лет
Срок реализации: 3 месяца

Составители программы:

Малыгин Александр Александрович,
педагог дополнительного образования.

Савельева Ольга Александровна,
методист.

Михайловск,
2020

ОГЛАВЛЕНИЕ

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

У человека всегда были две неотъемлемые потребности — (а) общаться и обмениваться информацией и (б) общаться избирательно. Эти две потребности породили искусство кодирования сообщений таким образом, чтобы только предполагаемые люди могли иметь доступ к информации. Несанкционированные люди не могли извлечь какую-либо информацию, даже если зашифрованные сообщения попали в их руки.

Искусство и наука сокрытия сообщений для обеспечения секретности в информационной безопасности названы криптографией. Слово «криптография» было придумано путем объединения двух греческих слов: «крипто» означает скрытый и «графен» означает письменность.

В течение многих лет криптография служила исключительно военным целям. Сегодня обычные пользователи получают возможность обращаться к средствам, позволяющим им обезопасить себя от несанкционированного доступа к конфиденциальной информации, применяя методы компьютерной криптографии.

Поэтому очень важно уметь ориентироваться в огромном объеме информации и особенно защищать ее криптографическими методами шифрования.

Направленность программы

Программа носит междисциплинарный характер и позволяет решить задачи развития у учащихся научно-исследовательских и практико-ориентированных компетенций.

Актуальность программы

Во все времена люди пытались скрыть ту или иную информацию от других. По мере развития цивилизации информации становилось всё больше, а необходимость её защитить от посторонних всё важнее и труднее.

Данная программа знакомит учащихся с основами и практикой защиты информации с помощью криптографических средств, что, как сказано выше, является в современном мире очень полезным и актуальным навыком.

Новизна программы

Если есть желающие скрыть смысл текста, то найдутся и желающие его прочитать. Сегодня защита информации одна из самых технологичных и засекреченных областей современной науки, которую изучают только в высших учебных заведениях. Однако её изучение было бы полезно и для старшеклассников, как углубленное изучение информатики и математики, так и с целью профессиональной ориентации в сфере информационной безопасности. Но подобных курсов среди образовательных программ школ нет. Именно в этом и состоит новизна данного курса.

Цель программы:

Формирование знаний и навыков, необходимых для обеспечения информационной безопасности с использованием шифровальных (криптографических) средств в информационных системах.

Задачи:

Образовательные:

• сформировать у учащихся представление о структуре и типах информации в интернет-пространстве;

• овладеть основными криптографическими инструментами, необходимыми для построения защищенных информационных систем;

• ознакомить учащихся с основами исследовательской деятельности (принципами построения исследования, процедурой и этикой его проведения, количественными и качественными методами обработки полученных данных).

Воспитательные:

• сформировать у учащихся культуру позитивного использования интернет-пространства;

• в защищенной среде продемонстрировать учащимся возможные угрозы и риски интернет-пространства;

• привить информационную культуру: ответственное отношение к информации с учетом правовых и этических аспектов её распространения, избирательного отношения к полученной информации.

Развивающие:

• сформировать у учащихся способность выявлять и критически оценивать источники и каналы распространения информации в интернет-пространстве и определять ее качество;

• сформировать у учащихся навыки планирования, проведения и обработки результатов исследования информации в интернет-пространстве при помощи поисковых систем;

• развивать познавательные способности ребенка, память, внимание, пространственное мышление, аккуратность и изобретательность.

Отличительные особенности программы

Основная особенность курса — изложение ведется без привлечения специальных и достаточно сложных разделов теории алгоритмов, но при этом все основные идеи и методы современной криптографии излагаются в полном объеме и без усложнения.

Программа направлена на формирование у учащихся базовых компетенций в области анализа информации и криптографии.

Категория обучающихся

Программа предназначена для детей, проявляющих интерес к информационным технологиям, стремящихся к саморазвитию, профессиональному самоопределению.

Возраст обучающихся: 13 - 17 лет.

Наполняемость группы: 10 человек.

Состав группы: разновозрастной.

Условия приема детей: на курсы программы зачисляются все желающие при наличии свободных мест.

Срок реализации программы: 3 месяца.

Структура программы:

Данный курс состоит из 13 тем.

1. Основы кодирования информации.
2. Основы информационной безопасности.

3. Введение в криптографию.
4. Шифры замены.
5. Шифры перестановки.
6. Шифры гаммирования.
7. Алгоритмы шифрования DES и AES.
8. Алгоритм RSA.
9. Криптографическая хеш-функция.
10. Криптографические протоколы.
11. Протокол электронно-цифровой подписи.
12. Криптоанализ.
13. Стеганография.

Форма реализации программы — смешанная / дистанционная с использованием электронного обучения.

Под электронным образованием понимается реализация образовательных программ с использованием информационно - образовательных ресурсов, информационно-коммуникационных технологий, технических средств, а также информационно-телекоммуникационных сетей, обеспечивающих передачу информационно-образовательных ресурсов и взаимодействие участников образовательного пространства.

Формы организации деятельности обучающихся

При изучении тем программа предусматривает использование фронтальной, индивидуальной и групповой формы учебной работы обучающихся, в том числе:

- интерактивные лекции;
- практическая работа;
- самостоятельная работа учащихся (индивидуально и в малых группах).

Методы обучения

При реализации программы рекомендуется использовать следующие методы:

- проблемное изложение;
- демонстрация наглядного материала;
- изучение источников;
- беседа;
- частично-поисковый (эвристический) метод;
- исследовательский метод;
- устный опрос.

Типы занятий: теоретические, практические, комбинированные, самостоятельные.

Режим занятий: два часа один раз в неделю.

Ожидаемые результаты

В результате освоения программы обучающийся должен приобрести следующие знания, умения и навыки:

знать:

✓ структуры интернет-пространства, типы источников информации и разновидностей контента;

✓ основы информационной безопасности;

✓ основы кодирования информации;

✓ различные криптографические алгоритмы;

уметь:

✓ работать с поисковыми системами, общедоступными средствами поиска информации в интернет-пространстве;

✓ анализировать информацию в интернет-пространстве при помощи количественных и качественных методов;

✓ решать задачи с применением криптографических методов;

✓ ставить цели, планировать свою работу и следовать намеченному плану, критически оценивать достигнутые результаты;

✓ свободно ориентироваться в интернет-пространстве, использовать различные типы источников для решения собственных задач;

обладать навыками:

✓ аналитического, практического и логического мышления;

✓ работы в команде;

✓ представления результатов своей работы окружающим, аргументирования своей позиции.

Способы определения результативности

Педагогическое наблюдение, педагогический анализ результатов решения практических задач по шифрованию данных.

Виды контроля:

- устный опрос;
- самостоятельная работа.

Формы подведения итогов реализации программы

По окончании обучения проводится итоговая аттестация в форме тестирования. Документальной формой подтверждения итогов аттестации является документ об образовании установленного Центром «Поиск» образца.

УЧЕБНО-ТЕМАТИЧЕСКИЙ ПЛАН

ПРОГРАММЫ «ШИФРОВАНИЕ ДАННЫХ»

№	Наименование темы	Количество часов		
		Теория	Практика	Всего
1.	Основы кодирования информации	1	1	2
2.	Основы информационной безопасности	2	0	2
3.	Введение в криптографию	2	0	2
4.	Шифры замены	1	0	1
5.	Шифры перестановки	1	1	2
6.	Шифры гаммирования	1	1	2
7.	Алгоритмы шифрования DES и AES	2	1	3
8.	Алгоритм RSA	2	1	3
9.	Криптографическая хеш-функция	1	1	2
10.	Криптографические протоколы	1	0	1
11.	Протокол электронно-цифровой подписи	1	1	2
12.	Криптоанализ	1	0	1
13.	Стеганография	1	0	1
	Итого	**17**	**7**	**24**

СОДЕРЖАНИЕ ПРОГРАММЫ
«ШИФРОВАНИЕ ДАННЫХ»

Тема 1. Основы кодирования информации.

Теория Основы кодирования информации. Цели кодирования

Практика. Способы кодирования.

Тема 2. Основы информационной безопасности.

Теория. Основы информационной безопасности. Виды угроз.

Тема 3. Введение в криптографию.

Теория. Базовые криптографические понятия, схемы, алгоритмы.

Тема 4. Шифры замены.

Теория. Различные шифры замены. Однозначная, многозначная замена.

Тема 5. Шифры перестановки.

Теория. Различные шифры перестановки. Шифры одинарной, множественной перестановки.

Практика. Решение задач по перестановке.

Тема 6. Шифры гаммирования.

Теория. Различные шифры гаммирования.

Практика. Различные задачи по гаммированию.

Тема 7. Алгоритмы шифрования DES и AES.

Теория. Алгоритмы шифрования DES и AES, основные сведения.

Практика. Различные задачи шифрования DES и AES.

Тема 8. Алгоритм RSA.

Теория. Алгоритм RSA, основные сведения.

Практика. Различные задачи с алгоритмом RSA.

Тема 9. Криптографическая хеш-функция.

Теория. Криптографическая хеш-функция. Применение хеш-функций для проверки истинности сообщений.

Практика. Различные задачи с хеш-функцией

Тема 10. Криптографические протоколы.

Теория. Криптографические протоколы. Основные понятия. Свойства безопасности протоколов.

Тема 11. Протокол электронно-цифровой подписи.

Теория. Протокол электронно-цифровой подписи. Общие сведения. Юридические основания использования ЭЦП.

Практика. Различные задачи по ЭЦП.

Тема 12. Криптоанализ

Теория. Криптоанализ. Основные сведения.

Тема 13. Стеганография

Теория. Стеганография. Стеганография в современных кибератаках.

Форма подведения итогов: итоговый тест, охватывающий все пройденные темы.

МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

ПРОГРАММЫ «ШИФРОВАНИЕ ДАННЫХ»

Тема занятия	Форма занятия	Приёмы и методы организации образовательного процесса	Дидактический материал. Электронные источники	Техническое оснащение и расходный материал	Форма подведения итогов
Основы кодирования информации	Комбинированная	Объяснительно-иллюстративный. Метод мозгового штурма. Проблемно-поисковый.	• Горев, А И; Симаков А А Обеспечение Информационной Безопасности / А Горев А И; Симаков А. - Москва: ИЛ, 2018.	● ПК / Ноутбуки с мышкой, наушниками, веб-камерой и доступом к сети Интернет. ● Презентационное оборудование.	Устный опрос
Основы информационной безопасности	Теоретическая	Объяснительно-иллюстративный.	• Горев, А И; Симаков А А Обеспечение Информационной Безопасности / А Горев А И; Симаков А. - Москва: ИЛ, 2018.	● ПК / Ноутбуки с мышкой, наушниками, веб-камерой и доступом к сети Интернет. ● Презентационное оборудование.	Устный опрос
Введение в криптографию	Теоретическая	Объяснительно-иллюстративный.	• Бабаш, А. В. История криптографии. Часть I / А.В. Бабаш, Г.П. Шанкин. - М.: Гелиос АРВ, 2017.	● ПК / Ноутбуки с мышкой, наушниками, веб-камерой и доступом к сети Интернет. ● Презентационное оборудование.	Тестирование
Шифры замены	Комбинированная	Объяснительно-иллюстративный.	• Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы. / Б. Шнайер. - М.: Триумф, 2017.	● ПК / Ноутбуки с мышкой, наушниками, веб-камерой и доступом к сети Интернет. ● Презентационное оборудование.	Тестирование
Шифры перестановки	Комбинированная	Объяснительно-иллюстративный. Метод мозгового	• Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы. / Б.	● ПК / Ноутбуки с мышкой, наушниками, веб-камерой и доступом к сети Интернет.	Тестирование

		штурма. Проблемно-поисковый.	Шнайер. - М.: Триумф, 2017. Кузьмин, Т. В. Криптографические методы защиты информации: моногр. / Т.В. Кузьмин. - Москва: Огни, 2018.	● Презентационное оборудование.	
Шифры гаммирования	Комбинированная	Объяснительно-иллюстративный. Метод мозгового штурма. Проблемно-поисковый.	• Р. Черчхаус Коды и шифры. Юлий Цезарь, "Энигма" и Интернет / Р. Черчхаус. - М.: Весь Мир, 2016. Кузьмин, Т. В. Криптографические методы защиты информации: моногр. / Т.В. Кузьмин. - Москва: Огни, 2018.	● ПК / Ноутбуки с мышкой, наушниками, веб-камерой и доступом к сети Интернет. ● Презентационное оборудование.	Тестирование
Алгоритмы шифрования DES и AES	Комбинированная	Объяснительно-иллюстративный. Метод мозгового штурма. Проблемно-поисковый.	• Р. Черчхаус Коды и шифры. Юлий Цезарь, "Энигма" и Интернет / Р. Черчхаус. - М.: Весь Мир, 2016. Кузьмин, Т. В. Криптографические методы защиты информации: моногр. / Т.В. Кузьмин. - Москва: Огни, 2018.	● ПК / Ноутбуки с мышкой, наушниками, веб-камерой и доступом к сети Интернет. ● Презентационное оборудование.	Устный опрос
Алгоритм RSA	Комбинированная	Объяснительно-иллюстративный. Метод мозгового штурма. Проблемно-поисковый.	• Р. Черчхаус Коды и шифры. Юлий Цезарь, "Энигма" и Интернет / Р. Черчхаус. - М.: Весь Мир, 2016. Кузьмин, Т. В. Криптографические методы защиты информации: моногр. / Т.В. Кузьмин. -	● ПК / Ноутбуки с мышкой, наушниками, веб-камерой и доступом к сети Интернет. ● Презентационное оборудование.	Тестирование

			Москва: Огни, 2018.		
Криптографическая хеш-функция	Комбинированная	Объяснительно-иллюстративный. Метод мозгового штурма. Проблемно-поисковый.	• Кузьмин, Т. В. Криптографические методы защиты информации: моногр. / Т.В. Кузьмин. - Москва: Огни, 2018.	● ПК / Ноутбуки с мышкой, наушниками, веб-камерой и доступом к сети Интернет. ● Презентационное оборудование.	Тестирование
Криптографические протоколы	Теоретическая	Объяснительно-иллюстративный.	• Кузьмин, Т. В. Криптографические методы защиты информации: моногр. / Т.В. Кузьмин. - Москва: Огни, 2018.	● ПК / Ноутбуки с мышкой, наушниками, веб-камерой и доступом к сети Интернет. ● Презентационное оборудование.	Устный опрос
Протокол электронно-цифровой подписи	Комбинированная	Объяснительно-иллюстративный. Метод мозгового штурма. Проблемно-поисковый.	Кузьмин, Т. В. Криптографические методы защиты информации: моногр. / Т.В. Кузьмин. - Москва: Огни, 2018.	● ПК / Ноутбуки с мышкой, наушниками, веб-камерой и доступом к сети Интернет. ● Презентационное оборудование.	Устный опрос
Криптоанализ	Теоретическая	Объяснительно-иллюстративный.	Кузьмин, Т. В. Криптографические методы защиты информации: моногр. / Т.В. Кузьмин. - Москва: Огни, 2018.	● ПК / Ноутбуки с мышкой, наушниками, веб-камерой и доступом к сети Интернет. ● Презентационное оборудование.	Решение задач
Стеганография	Комбинированная	Объяснительно-иллюстративный. Метод мозгового штурма. Проблемно-поисковый.	• Грибунин Вадим Геннадьевич «Цифровая стеганография» / Грибунин Вадим Геннадьевич. - М.: Солон-Пресс, 2016.	● ПК / Ноутбуки с мышкой, наушниками, веб-камерой и доступом к сети Интернет. ● Презентационное оборудование.	Итоговый тест

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

- Грибунин Вадим Геннадьевич «Цифровая стеганография» / Грибунин Вадим Геннадьевич. - М.: Солон-Пресс, 2016.
- Бабаш, А. В. История криптографии. Часть I / А.В. Бабаш, Г.П. Шанкин. - М.: Гелиос АРВ, 2017.
- Горев, А И; Симаков А А Обеспечение Информационной Безопасности / А Горев А И; Симаков А. - Москва: ИЛ, 2018.
- Кузьмин, Т. В. Криптографические методы защиты информации: моногр. / Т.В. Кузьмин. - Москва: Огни, 2018.
- Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы. / Б. Шнайер. - М.: Триумф, 2017.
- Бузов, Геннадий Алексеевич «Защита информации ограниченного доступа от утечки по техническим каналам» / Бузов Геннадий Алексеевич. - М.: Горячая линия - Телеком, 2019.
- Р. Черчхаус Коды и шифры. Юлий Цезарь, "Энигма" и Интернет / Р. Черчхаус. - М.: Весь Мир, 2016.