|  |  |  |
| --- | --- | --- |
|  **«Рассмотрено»**на заседании ШМОПротокол № \_\_\_\_\_\_\_\_\_\_\_\_\_\_от «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_2014г. Руководитель ШМО\_\_\_\_\_\_\_\_\_\_\_\_/ Т.А.Хмелькова/ | **«Согласовано»**«\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_2014г. Зам. директора по УВР МОУ «СОШ № 1 г. Ершова»\_\_\_\_\_\_\_\_\_\_\_\_/И.В. Рябинцева/ | **«Утверждаю»**Приказ №\_\_\_\_\_\_\_\_\_\_\_ от «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_2014г.Директор МОУ «СОШ № 1 г. Ершова»\_\_\_\_\_\_\_\_\_\_\_\_\_/Г.Н. Лепёхин/ |

**РАБОЧАЯ ПРОГРАММА**

**Элективного курса по информатике**

 **«Криптографические основы безопасности»**

**для 10-11-х классов**

**МОУ «Средняя общеобразовательная школа № 1**

**города Ершова Саратовской области»**

**Составитель**:

 Арутюнян Лилит Эдуардовна,

 учитель информатики и ИКТ

Принято на заседании

педагогического совета

протокол № \_\_\_\_от

 «\_\_\_\_\_\_»\_\_\_\_\_\_\_20\_\_\_\_\_г.

**г. Ершов**

**2014г.**

 Рабочая программа элективного курса информатике «Криптографические основы безопасности» для 10-11-х классовучебного плана Муниципального образовательного учреждения «Средняя образовательная школа № 1 города Ершова Саратовской области».

На реализацию программы необходимо 2года.

**Криптографическая защита информации** история криптографии; классические шифры, шифры гаммирования и колонной замены; простейшие шифры и их свойства; системы шифрования с открытым ключом; криптографическая стойкость шифров; модели шифров; основные требования к шифрам; вопросы практической стойкости; имитостойкость и помехоустойчивость шифров; принципы построения криптографических алгоритмов; различия между программными и аппаратными реализациями; криптографические параметры узлов и блоков шифраторов; синтез шифров; методы получения случайных и псевдослучайных последовательностей; программные реализации шифров; особенности использования вычислительной техники в криптографии; вопросы организации сетей засекреченной связи; ключевые системы; криптографические хеш-функции; электронная цифровая подпись; криптографические протоколы.

**1. Цели и задачи учебной дисциплины, ее место в учебном процессе**

**1.1. Цели и задачи дисциплины**

Цель курса – сформировать представление о современных методах и средствах криптографической защиты информации, используемых, в частности, для решения проблем компьютерной безопасности.

В результате изучения курса студенты должны овладеть основным криптографическим инструментарием, необходимым для построения защищенных информационных систем.

Предметом курса является изложение основ криптографической защиты информации, ее применение в современных информационных технологиях.

Содержание курса: математические модели криптоалгоритмов (теоретико-численные основы криптологии), симметрические и ассиметрические криптосистемы, понятие и методы построения хэш-функций, стандарты шифрования (отечественные и зарубежные), алгоритмы аутентификации и идентификации, их применение в корпоративных сетях и банковских технологиях (смарт-карты, сложные платежные системы, электронные деньги), проблемы распределения открытых и секретных ключей, протоколы распределения ключей.

В результате изучения дисциплины студенты должны иметь представление о роли математики, ее месте в криптографии и методах решения задач криптоанализа, о методах криптоанализа.

**Учащиеся должны:**

**знать:**

- криптоалгоритмы, используемые в современных криптосистемах с открытым ключом;

- криптоалгоритмы, используемые в стандартах шифрования данных;

- методы выбора криптографических параметров, обеспечивающих необходимую стойкость криптосистемы;

 - ключевые системы современных криптосистем и протоколы распределения ключей;

- приложения криптографии к решению различных проблем защиты информации в компьютерных системах и сетях, проблемы безопасности электронных банковских систем;

**уметь:**

- применять полученные знания к исследованию простых шифров;

- строить и изучать математические модели криптоалгоритмов;

- решать основные задачи на применение криптографических алгоритмов в защите информации;

**владеть навыками:**

- применения отечественной и зарубежной терминологии в области криптографии для выражения количественных и качественных требований по защите информации;

- использования математического аппарата в проведении исследований;

- использования данных Интернет-ресурсов;

- использования компьютерных технологий при решении прикладных программ.

**1.2. Краткая характеристика дисциплины, ее место в учебном процессе**

Криптографическая защита информации – дисциплина, изучающая средства, схемы, способы и многочисленные возможности обеспечения криптографической защиты важной информации, имеющей отношение к деятельности и взаимосвязям данного конкретного предприятия и/или сети. Вопросы данного предмета оказываются важными при прохождении студентами производственной практики, а также при написании дипломных или квалификационных работ. Изучение основ, теории и нормативно-правовой базы криптографической защиты информации, правильное объяснение работы информационных потоков и использование средств улучшения работы путем налаживания криптографически безопасной информационной инфраструктуры и внедрения инновационных физических и административных мер обеспечивает студентам дополнительные возможности при работе по специальности.

**1.3. Связь с предшествующими и последующими дисциплинами**

В курсе «Криптографические основы безопасности» студенты знакомятся с системой защиты информации, включающей в себя знания по созданию и поддержанию надежных и безопасных криптосистем, приобретению и использованию физических средств контроля и защиты информационных носителей от криптоанализа, новейшими компьютерными технологиями в области криптографической защиты. Внимание уделяется взаимосвязи криптографии и математики, крупный раздел которой (теория чисел) изучается в рамках данной дисциплины, а также ПАЗИ, средства которые представляют собой схемы криптоалгоритмов и/или содержат ПО, созданное с использованием основ криптографии.

**3. Содержание дисциплины**

**3.1. Лекционный курс**

|  |  |  |
| --- | --- | --- |
| Порядковый номер лекции | Раздел, тема учебного курса, содержание лекции | Кол-во часов |
| **РАЗДЕЛ I. ВВЕДЕНИЕ. КЛАССИЧЕСКИЕ ШИФРЫ** |
| 1-2. | История криптографии. Определение шифра. Классические шифры, шифры гаммирования и колонной замены. Простейшие шифры и их свойства. Композиции шифров. Системы шифрования с открытыми ключами. | 2 |
| 3-4 | Криптографическая стойкость шифров. Модели шифров. Основные требования к шифрам. Вопросы практической стойкости; имитостойкость и помехоустойчивость шифров. Принципы построения криптографических шифров. | 2 |
| 5-6 | Понятие криптографического алгоритма. Принципы построения криптографических алгоритмов. Различие между программными и аппаратными реализациями. Криптографические параметры узлов и блоков шифраторов. Синтез шифров. Методы получения случайных и псевдослучайных последовательностей. Программные реализации шифров. Криптосистемы с открытым ключом. Функции хэширования. Хэш-код. Криптопротоколы. | 2 |
| 7-8 | Понятие поточных шифров. Их классификация. Синхронные поточные шифры. Самосинхронизирующиеся поточные шифры. | 2 |
| 9-10 | Нелинейная комбинация генераторов. Генератор, управляемый часами. Методы получения случайных и псевдослучайных последовательностей. | 2 |
| 11-12 | Анализ генератор псевдослучайных чисел. Роторные (барабанные) шифровальные машины. | 2 |
| 13-14 | Понятие блочных шифров. Примеры схем блочных шифров. Шифры перестановки и подстановки. Моноалфавитные и полиалфавитные подстановочные шифры. | 2 |
| 15-16 | Режимы использования блочных шифров. Электронная кодовая книга. Отечественный стандарт шифрования данных ГОСТ 28147-89 | 2 |
| 17-18 | Американский стандарт шифрования данных DES. История его разработки, свойства, режимы использования. Тройной DES. | 2 |
| 19-20 | Особенности использования вычислительной техники в криптографии. Ключевые системы. | 2 |
| 21-22 | Принципы построения криптосистем с открытым ключом. Применение криптосистем с открытым ключом. Условия применения методов криптографии с открытым ключом. Криптоанализ схем шифрования с открытым ключом. | 2 |
| 23-24 | Алгоритм RSA. Описание алгоритма. Вычислительные аспекты. Защищенность алгоритма RSA. Атаки на RSA. | 2 |
| 25-26 | Управление ключами. Распределение открытых ключей. Распределение секретных ключей с помощью системы с открытым ключом. | 2 |
| 27-28 | Система Диффи-Хеллмана. Вопросы организации сетей засекреченной связи. Схема шифрования El-Gamal. Подпись El-Gamal. | 2 |
| 29-30 | Электронная цифровая подпись. Криптографические хэш-функции. Криптографические протоколы. Классификация атак на электронную подпись. | 2 |
| 31-32 | Аутентификация, авторизация, аудит. Схема Kerberos. История создания, описание схемы, применение в криптографической ЗИ. | 2 |
| 33-34 | Простые и взаимно простые числа. Арифметика в классах вычетов. Теоремы Ферма и Эйлера. Проверка числа на простоту. | 2 |
| 35-36 | Алгоритм Евклида. Китайская теорема об остатках. Дискретные логарифмы. | 2 |
|  | **Итого:** | **36** |

**3.3. Лабораторные работы**

|  |  |  |  |
| --- | --- | --- | --- |
| Номер лаб. работы | Наименование лабораторной работы | Раздел, тема лекционного курса | Объем часов |
| 1-4. | Основные понятия, термины и определения криптологии. Криптография и криптоанализ шифра Цезаря. Требования к шифрам. Ключевые системы. Криптографические хэш-функции. Электронная цифровая подпись. Криптографические протоколы. | I-1,2,3 | 4 |
| 5-8 | Поточные шифры. Барабанные машины. Шифр и табло Виженера. Шифрование, дешифрование, криптоанализ. | II-4,5,6 | 4 |
| 9-12 | Шифр Вернама. Шифрование, дешифрование, криптоанализ. | II-4,5,6 | 4 |
| 13-16 | ГОСТы. Нормативно-правовая база криптографии. DES. Тройной DES. | III-8,9 | 4 |
| 17-21 | Дифференциальный и линейный криптоанализ блочных шифров. | III-9 | 5 |
| 22-26 | Криптосистемы с открытым ключом. Алгоритм RSA. | IV-10,11 | 5 |
| 27-30 | Управление ключами. Система Диффи-Хеллмана. | IV-12,13 | 4 |
| 31-34 | Схема шифрования Еl-Gamal. Схема Kerberos. | IV-15,16 | 4 |
|  | **Итого:** |  | **34** |

**3.4. Содержание и объем самостоятельной работы учащихся**

Внеаудиторная самостоятельная работа студентов включает следующие виды деятельности:

- конспектирование первоисточников и другой учебной литературы;

- переработку учебного материала (по конспектам, учебной и научной литературе);

- изучение учебного материала, перенесенного с аудиторных занятий на самостоятельную проработку;

- написание рефератов;

- выполнение расчетно-графических домашних заданий;

- решение задач и упражнений;

- подготовку к зачету.

**3.5. Организация и методика текущего и итогового контроля знаний**

|  |  |  |
| --- | --- | --- |
| Перечень контрольных работ, тестов | Сроки проведения контроля | Разделы и темы рабочей программы |
| Самостоятельная работа №1 | I полугодие | Разделы I- III Все темы |
| Контрольная работа | I полугодие | Разделы I- III Все темы |
| Самостоятельная работа №2 | II полугодие | Раздел V Все темы  |
| Контрольная работа | II полугодие | Разделы I-V Все разделы |

**4.1. Основная и дополнительная литература**

**Основная литература**

1. ЭБС «Айбукс» **Бабаш, А. В.** Криптографические и теоретико-автоматные аспекты современной защиты информации. Криптографические методы защиты. Том 3: учеб. пособие — М. : ЕАОИ, 2011. — 215 с. Режим доступа: <http://ibooks.ru/>

1. Черемушкин, А.В. Криптографические протоколы. Основные свойства и уязвимости : учеб. пособие для студентов вузов / А.В. Черемушкин. - М. : Академия, 2009. - 272 с.

**3.** ЭБС «Айбукс» **Бабаш, А. В.** Криптографические и теоретико-автоматные аспекты современной защиты информации. Криптографические методы защиты. Том 2.: учеб. пособие — М. : ЕАОИ, 2008. — 257 с. - Режим доступа: <http://ibooks.ru/>

**Дополнительная литература**

1. Рябко, Б.Я. Криптографические методы защиты информации : учеб. пособие для студентов вузов / Б.Я. Рябко, А.Н. Фионов. - М. : Горячая линия - Телеком, 2005. - 229 с. :

2. Левин, М.. Криптография без секретов : руководство пользователя / М. Левин. - М. : Новый издательский дом, 2005. - 320 с.