ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ ГОРОДА МОСКВА

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ

СРЕДНЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ ГОРОДА МОСКВЫ

КОЛЛЕДЖ СВЯЗИ №54

**рабочая ПРОГРАММа**

УЧЕБНОЙ ДИСЦИПЛИНЫ **ОП.13. Математические основы защиты информации**

СПЕЦИАЛЬНОСТЬ **090905 Организация и технология защиты информации**

по программе базовой подготовки

на базе среднего (полного) общего образования

Москва

2014

|  |  |
| --- | --- |
| Рассмотрена | Разработана на основе Федерального |
| Предметной (цикловой) | государственного образовательного |
| комиссией ОП | стандарта по специальности среднего |
| укрупненной группы 090000 | профессионального образования |
| Протокол №\_\_\_\_\_  от «\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_2014г. | 090905 Организация и технология защиты информации |
| Председатель предметной  (цикловой) комиссии | Заместитель директора по УМР |
| \_\_\_\_\_\_\_\_\_\_А.А.Юмаева | \_\_\_\_\_\_\_\_\_\_\_\_И.Г.Бозрова |
|  | «\_\_\_\_\_\_» \_\_\_\_\_\_\_ 2014г. |
|  |  |
|  |  |

**Разработали:** Е.Е. Сверчков, преподаватель ГБОУ СПО Колледж связи №54

# СОДЕРЖАНИЕ

|  |  |
| --- | --- |
|  | стр. |
| ПАСПОРТ рабочей ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ | 4 |
| СТРУКТУРА и содержание УЧЕБНОЙ ДИСЦИПЛИНЫ | 5 |
| условия реализации рабочей программы учебной дисциплины | 9 |
| Контроль и оценка результатов Освоения учебной дисциплины | 10 |

**1. паспорт рабочей ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ**

**Математические основы защиты информации**

**1.1. Область применения программы**

Рабочая программа учебной дисциплины является частью основной профессиональной образовательной программы в соответствии с ФГОС по специальности СПО 090905 Организация и технология защиты информации.

**1.2. Место учебной дисциплины в структуре основной профессиональной образовательной программы.**

Дисциплина входит в профессиональный цикл, как общепрофессиональная дисциплина вариативной части

**1.3. Цели и задачи дисциплины – требования к результатам освоения дисциплины:**

В результате освоения дисциплины обучающийся должен

**Уметь**:

* Разрабатывать алгоритмы защиты информации;
* Генерировать простые числа.

**Знать:**

* классические системы шифрования;
* алгоритмы шифрования;
* применение эллиптических кривых в криптографии. ПК и ОК, которые актуализируются при изучении учебной дисциплины:
* ОК 1. Понимать сущность и социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности.
* ОК 2. Организовывать собственную деятельность, определять методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.
* ОК 3. Решать проблемы, оценивать риски и принимать решения в нестандартных ситуациях.
* ОК 4. Осуществлять поиск, анализ и оценку информации, необходимой для постановки и решения профессиональных задач, профессионального и личностного развития.
* ОК 5. Использовать информационно-коммуникационные технологии для совершенствования профессиональной деятельности.
* ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.
* ОК 9. Быть готовым к смене технологий в профессиональной деятельности.
* ПК 1.6. Обес­пе­чи­вать тех­ни­ку безо­пас­но­сти при про­ве­де­нии ор­га­ни­за­ци­он­но-тех­ни­че­ских ме­ро­прия­тий.
* ПК 3.1. При­ме­нять про­грамм­но-ап­па­рат­ные и ин­же­нер­но-  
  тех­ни­че­ские сред­ст­ва за­щи­ты ин­фор­ма­ции на объ­ек­тах про­фес­сио­наль­ной дея­тель­но­сти.
* ПК 3.2. Уча­ст­во­вать в экс­плуа­та­ции за­щи­щен­ных объ­ек­тов   
  про­фес­сио­наль­ной дея­тель­но­сти.
* ПК 3.3. Про­во­дить рег­ла­мент­ные ра­бо­ты и фик­си­ро­вать от­ка­зы средств

за­щи­ты.

* ПК 3.4. Вы­яв­лять и ана­ли­зи­ро­вать воз­мож­ные уг­ро­зы   
  ин­фор­ма­ци­он­ной безо­пас­но­сти объ­ек­тов.

**1.4. Рекомендуемое количество часов на освоение программы дисциплины:**

максимальной учебной нагрузки обучающегося **162 часа**, в том числе:

обязательной аудиторной учебной нагрузки обучающегося **108 часов;**

самостоятельной работы обучающегося **54 часа.**

**2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ**

**2.1. Объем учебной дисциплины и виды учебной работы**

|  |  |
| --- | --- |
| **Вид учебной работы** | ***Объем часов*** |
| **Максимальная учебная нагрузка (всего)** | ***162*** |
| **Обязательная аудиторная учебная нагрузка (всего)** | ***108*** |
| в том числе: |  |
| Практические занятия | ***20*** |
| **Самостоятельная работа обучающегося (всего)** | ***54*** |
| *Промежуточная аттестация в форме контрольной работы (5 семестр) и зачета (6 семестр)* |  |

## *2.2. Тематический план и содержание учебной дисциплины*

## *Математические основы защиты информации*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Наименование разделов и тем** | | **Содержание учебного материала, практические работы, самостоятельная работа обучающихся** | **Объем часов** | **Уровень освоения** |
| **1** | | **2** | **3** | **4** |
| **Раздел 1: Введение в информационную безопасность** | | | **16** |  |
| **Тема 1.1. Основы информационной безопасности** | | **Содержание учебного материала** | 6 | 2 |
| Основные понятия информационной безопасности. Конфиденциальность. Целостность. Доступность.  Методы информационной безопасности. Физические, организационно-правовые и технические средства защиты.  Сервисы информационной безопасности. Аутентификация, авторизация и аудит. |
| **Тема 1.2. Анализ угроз информационной безопасности** | | **Содержание учебного материала** | 4 | 2 |
| Угрозы информационной безопасности.  Классификация криптографических методов защиты информации |
| **Самостоятельная работа №1.** | 6 |  |
| 1.1. Подготовка презентации по теме «Угрозы информационной безопасности»  1.2. Составление конспекта по теме «Организационно-правовые средства защиты». |
| **Раздел 2. Системы шифрования с открытым ключом. Метод RSA.** | | | **86** |  |
| **Тема 2.1. Классические системы шифрования** | | **Содержание учебного материала** | 6 | 2 |
| Особенности систем с открытым ключом  Модулярная арифметика  Функция Эйлера φ(n) |
| **Тема 2.2. Алгоритмы шифрования** | | **Содержание учебного материала** | 6 | 2 |
| Алгоритм RSA  Расширенный алгоритм Евклида  Алгоритм быстрого возведения в степень по модулю |
| **Тема 2.3. Математические основы шифрования** | | **Содержание учебного материала** | 22 | 2 |
| Генерация простых чисел. Решето Эратосфена  Метод пробных делений  Решето Аткина  Тест Поклингтона  Обобщенная гипотеза Римана  Символ Лежандра  Тест простоты Миллера-Рабина  Вероятностный тест простоты Соловея-Штрассена  Полиноминальный критерий простоты AKS  Извлечение квадратного корня в конечных полях  Китайская теорема об остатках |
| **Практические занятия** | 12 |  |
| 1-2 Модулярная арифметика, функция Эйлера.  3-4 Алгоритм RSA, расширенный алгоритм Евклида  5-6 Метод пробных делений, генерация простых чисел |  |  |
| **Тема 2.4.**  **Криптостойкость RSA. Алгоритмы факторизации.** | | **Содержание учебного материала** | 16 |  |
| Метод Ферма  (р-1) метод Полларда  ρ – метод Полларда  (р-1) метод Вильямса  Метод Полларда для вычисления дискретного логарифма  Протокол Диффи-Хеллмана  Электронная цифровая подпись и ее свойства  *Контрольная работа* |
| **Самостоятельная работа №2.** | 24 |  |
| 2.1. Подготовка к практическим занятиям  2.2. Подготовка доклада по теме « Основы шифрования»  2.3. Подготовка презентации по теме «Электронная цифровая подпись» |
| **Раздел 3.** **Криптографические методы, основанные на задаче дискретного логарифмирования в конечном поле** | | | **12** |  |
| **Тема 3.1 Защита электронного документа** | **Содержание учебного материала** | | 6 | 2 |
| Односторонние функции. Хэш-функции  Алгоритм создания электронной цифровой подписи  Алгоритм построения ЭЦП Эль-Гамаля | |
| **Самостоятельная работа №3:**  3.1. Подготовка к практическим работам  3.2. Составление презентации по теме « Защита электронного документа» | | 6 |  |
| **Раздел 4. Эллиптические кривые и их приложения в криптографии.** | | | **48** |  |
| **Тема 4.1 Основные свойства эллиптических кривых** | **Содержание учебного материала** | | 8 | 2 |
| Определение эллиптической кривой  Эллиптические кривые в проективных координатах  Эллиптические кривые в якобиановых проективных координатах  Число точек эллиптической кривой | |
| **Тема 4.2 Методы факторизации** | **Содержание учебного материала** | | 6 | 2 |
| Алгоритм факторизации Ленстры ECF  Рекордные разложения метода ECFM  Метод Монтгомери | |
| **Практические занятия** | | 8 |  |
| 7-8 Хэш-функции  9-10 Эллиптические кривые. | |
| **Тема 4.3 Отображения Вейля и Тейта** | **Содержание учебного материала** | | 8 | 2 |
| Криптографические протоколы на эллиптических кривых  Дивизоры  Алгоритм Миллера  Зачетное занятие | |
|  | **Самостоятельная работа №4:**  4.1. Подготовка к практическим работам  4.2. Подготовка презентации по теме «Свойства эллиптических кривых»  4.3. Подготовка к зачету. | | 18 |  |
| **Всего** |  | | **162** |  |

# 

# 3. условия реализации рабочей программы дисциплины

**3.1. Требования к материально-техническому обеспечению**

Реализация рабочей программы дисциплины требует наличия учебного кабинета Информационной безопасности, оснащенного компьютерной техникой с установленным программным обеспечением.

Оборудование учебного кабинета: посадочные места, видеопроектор, интерактивная доска, электронные учебники по дисциплине.

**3.2. Информационное обеспечение обучения**

**Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы**

**Основные источники:**

1. Анин Б. Ю. Защита компьютерной информации. - СПб.: БХВ-Петербург, 2010
2. Ишмухаметов Ш.Т., Рубцова Р.Г. Математические основы защиты информации. Электронное учебное пособие.- Казань, 2012
3. Чмора А. Л. Современная прикладная криптография.- М.: Гелиос АРВ, 2011

**Дополнительные источники:**

1. Романов И. Л. Алгоритмы криптографического преобразования.-СПб.: БВХ-Петербург, 2013
2. Безопасность компьютерных сетей на основе Windows NT Люцарев В.С. М.: Русская редакция, 2011

**Интернет ресурсы:**

1. <http://life-prog.ru/view_zam2.php?id=228&cat=5&page=17>.
2. <http://window.edu.ru/resource/651/45651/files/unn078.pdf>
3. http://e-college.ru/xbooks/xbook010/book/index/index.html?go=part-011\*page.htm
4. http://coolreferat.com
5. http://www.e-college.ru/xbooks/xbook010/book/index/index.html?go=part-012\*page.htm
6. http://window.edu.ru/window/library/pdf2txt?p\_id=53723&p\_page=2
7. http://topknowledge.ru/index.php?option=com\_content&view

**4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ**

# Контроль и оценка результатов освоения дисциплины осуществляется преподавателем в процессе проведения практических занятий, тестирования, а также выполнения обучающимися индивидуальных заданий, исследований.

|  |  |
| --- | --- |
| **Результаты обучения (освоенные умения, усвоенные знания)** | **Формы и методы контроля и оценки результатов обучения** |
| ***Освоенные умения:***  Разрабатывать алгоритмы защиты информации;  Генерировать простые числа. | *Экспертная оценка результатов деятельности студентов при выполнении и защите практических работ выполнения самостоятельной работы. Наблюдение за студентами во время выполнения ими индивидуальных заданий.* |
| ***Усвоенные знания:***  классических систем шифрования;  алгоритмов шифрования;  применения эллиптических кривых в криптографии | *Экспертная оценка результатов деятельности студентов при выполнении и защите практических работ, тестирования, зачета.* |