**ПРОГРАММа УЧЕБНОЙ ДИСЦИПЛИНЫ**

**КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ**

(БАЗОВЫЙ УРОВЕНЬ)

2012 г.

Рабочая программа учебной дисциплины Криптографические методы защиты информации разработана на основе Федерального государственного образовательного стандарта (далее – ФГОС) по специальности среднего профессионального образования (далее СПО) базовой подготовки 090905 Организация и технология защиты информации.

Организация-разработчик: ОГБОУ СПО «Смоленский промышленно-экономический колледж»

Разработчики:

Малахова В.Г., преподаватель ОГБОУ СПО «Смоленский промышленно-экономический колледж»

Утверждена Научно-методическим советом ОГБОУ СПО «Смоленский промышленно-экономический колледж»

Протокол № 1 от 11.09.2012 г.

Рассмотрена на заседании кафедры

Протокол № 1 от 30.08.2012 г.

# **СОДЕРЖАНИЕ**

|  |  |
| --- | --- |
|  | стр. |
| **ПАСПОРТ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ** | 3 |
| **Результаты освоения учебной дисциплины** | 4 |
| **СТРУКТУРА и ПРИМЕРНОЕ содержание УЧЕБНОЙ ДИСЦИПЛИНЫ** | 5 |
| **условия реализации программы учебной дисциплины** | 11 |
| **Контроль и оценка результатов Освоения учебной дисциплины** | 12 |

**1. паспорт ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ**

**Криптографические методы защиты информации**

**1.1. Область применения программы**

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

**1.2. Место дисциплины в структуре основной профессиональной образовательной программы:** дисциплина входит в общепрофессиональный цикл.

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

В результате освоения дисциплины обучающийся должен уметь:

Использовать программно-аппаратные средства для обработки шифрованных данных

Рассчитывать параметры типовых шифров замены и перестановки;

Использовать частотные характеристики языков в криптоанализе;

В результате освоения дисциплины обучающийся должен знать:

Место и роль криптографических методов в системах защиты государственной, конфиденциальной и коммерческой информации

Требования к шрифтам и основные характеристики шрифтов;

Принципы построения современных шифросистем;

Основные математические методы, используемые в анализе типовых криптографических алгоритмов

Криптографические протоколы;

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

максимальной учебной нагрузки обучающегося 96 часов/ 3 зачетные ед., в том числе:

обязательной аудиторной учебной нагрузки обучающегося 64 часа;

самостоятельной работы обучающегося 32 часа.

**2. Результаты освоения учебной дисциплины**

Результатом освоения учебной дисциплины Криптографические методы защиты информации является овладение общими (ОК) компетенциями:

|  |  |
| --- | --- |
| **Код** | **Наименование результатов обучения** |
| 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, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество. |
| ОК 3. | Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность. |
| ОК 4. | Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития. |
| ОК 5. | Использовать информационно-коммуникационные технологии в профессиональной деятельности. |
| ОК 6. | Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями. |
| ОК 7. | Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий. |
| ОК 8. | Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации. |
| ОК 9. | Ориентироваться в условиях частой смены технологий в профессиональной деятельности. |
| ОК 10. | Исполнять воинскую обязанность, в том числе с применением полученных профессиональных знаний (для юношей). |
| ОК 11. | Применять математический аппарат для решения профессиональных задач. |
| ОК 12. | Оценивать значимость документов, применяемых в профессиональной деятельности. |
| ОК 13. | Ориентироваться в структуре федеральных органов исполнительной власти, обеспечивающих информационную безопасность. |
| ПК 2.3. | Организовывать документооборот, в том числе электронный, с учетом конфиденциальности информации. |
| ПК 2.9. | Использовать нормативные правовые акты, нормативно-методические документы по защите информации. |
| ПК 3.1. | Применять программно-аппаратные и технические средства защиты информации на защищаемых объектах. |

**3. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ**

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

|  |  |
| --- | --- |
| **Вид учебной работы** | ***Объем часов*** |
| **Максимальная учебная нагрузка (всего)** | 96 |
| **Обязательная аудиторная учебная нагрузка (всего)** | 64 |
| в том числе: |  |
| практические занятия | 24 |
| семинарские занятия | 38 |
| контрольные работы | 1 |
| дифференцированный зачет | 1 |
| **Самостоятельная работа обучающегося (всего)** | 32 |
| *Выполнение упражнений*  *Выполнение индивидуального задания*  *Подготовка к контрольной работе, зачету* | *16*  *12*  *4* |
| Итоговая аттестация в форме***дифференцированного******зачёта*** | |

# **3.2. Примерный тематический план и содержание учебной дисциплины** **Криптографические методы защиты информации**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Наименование разделов и тем** | **Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работ (проект)** | | **Объем часов** | **Уровень освоения** |
| **1** | **2** | | **3** | **4** |
| **Раздел 1** | **История криптографии** | | ***36*** |  |
| **Тема 1.1. Введение в криптографию** | 1 | **Введение в предмет**  Роль и место знаний по дисциплине в сфере профессиональной деятельности. Понятие криптографии. История развития криптографии. Основные проблемы и перспективы развития криптографических систем. | ***2*** | *1* |
| 2 | **Основные принципы криптографии**   1. Шифр Цезаря. Уязвимости одноалфавитных замен. 2. Квадрат Полибия. 3. Квадрат Кардана. Шифры перестановки. 4. Таблица Виженера. Две качественно новых идеи шифрования. 5. Цифровая криптография. Шифр Вернама. Идея одноразового блокнота. | ***2*** | *1*  *2* |
| **Самостоятельная работа обучающихся**  Выполнение упражнений | | ***2*** | *2* |
| Тема 1.2. Классификация шифров | 1 | **Классификация по ключевой информации**   1. Симметричное/асимметричное шифрование. 2. Нелинейные поточные шифры. | ***2*** | *1* |
| 2 | **Основы блочного шифрования**   1. Основные идеи. 2. Обратимые операции в блочном шифровании. 3. Необратимые операции в блочном шифровании. 4. Сети. SP-сеть, KASLT-сеть, Сеть Фейстеля. | ***4*** | *1* |
| **Практические занятия** | | **4** |  |
| Шифры перестановки и замены | | ***2*** | *2,3* |
| Блочные составные шифры | | *2* |
| **Самостоятельная работа обучающихся**  Выполнение упражнений | | ***4*** | *2* |
| **Тема 1.3. Практика блочного шифрования** | 1 | **Общие принципы алгоритма DES**   1. Аппаратное шифрование: DES. 2. Эпоха пост- DES. Общие тенденции. 3. Блочный шифр ТЕА. 4. Алгоритм IDEA. | **2** | *1* |
| 2 | **Общие принципы алгоритма ГОСТ**   1. Алгоритм ГОСТ 28147-89. 2. Конкурс АЕS. | **2** | *1* |
|  |
| **Практические занятия** | | ***6*** | *2,3* |
| ***Тема: «Шифры моноалфавитной подстановки»***  Создать программу для дешифрования криптограмм, зашифрованных методом моноалфавитных подстановок, используя частотный анализ. | | ***2*** |
| ***Тема «Метод вероятных слов»***  1. Дешифровать криптограмму, зашифрованую шифром Виженера, методом вероятных слов, получить ключ шифрования;  2. Дешифровать криптограмму, зашифрованую "бегущим" ключом, методом вероятных слов, получить "бегущий" ключ. | | ***2*** |
| ***Тема «Шифр многопетлевой полиалфавитной подстановки»***  1. Определить период шифра предлагаемой криптограммы;  2. Дешифровать криптограмму и получить составной ключ;  3. Вычислить первичные ключи. | | ***2*** |
| **Самостоятельная работа обучающихся**  *Выполнение упражнений* | | ***6*** |
| **Раздел 2** | **Стандарты шифрования. Криптографическая стойкость** | | ***25*** |  |
| **Тема 2.1. Надежность шифров. Имитостойкость шифров. Помехоустойчивость шифров** | 1 | **Свойства шифров**   1. Оценка криптостойкости шифров. 2. Характеристика имитостойкости шифров. 3. Характеристики помехоустойчивости. 4. Надежность шифров. | ***4*** | *1* |
| **Практические занятия** | | ***4*** | *2,3* |
| ***Абсолютно стойкий шифр. Применение режима однократного гаммирования. Шифрование (кодирование) различных исходных текстов одним ключом*** | | *2* |
| ***Анализ методики многократного использования ключа и материала исходного блока информации (алгоритм DES)*** | | *2* |
| **Самостоятельная работа обучающихся**  *Выполнение индивидуального задания* | | ***4*** |
| **Тема 2.2. Принципы построения криптографических алгоритмов** | 1 | **Элементы криптоанализа**   1. Криптоанализ шифров перестановки. 2. Криптоанализ поточного шифра простой замены. 3. Криптоанализ шифра модульного гаммирования | ***4*** | *1* |
| **Практические занятия** | | ***4*** | *2,3* |
| ***Генерирование равномерно распределенных псевдослучайных последовательностей*** | | *2* |
| ***Методы криптографии. Генерация псевдобесконечных ключей на основе датчиков псевдослучайных чисел*** | | *2* |
| **Самостоятельная работа обучающихся**  *Выполнение индивидуального задания*  *Подготовка к контрольной работе* | | ***4*** |
|  | **Контрольная работа** | | ***1*** |  |
| **Раздел 3** | **Криптографические системы шифрования** | | ***35*** |  |
| **Тема 3.1. Шифры с открытыми ключами** | 1 | **Ассиметричное шифрование**   1. Алгоритм RSA. 2. Криптосхема Рабина 3. Алгоритм Эль Гамаля. 4. Принцип открытого распространения ключей. 5. Криптосистемы на эллиптических кривых. | ***6*** | *1* |
| **Практические занятия** | | ***4*** | *2,3* |
| ***Тестирование чисел на простоту и построение больших простых чисел*** | | *2* |
| ***Факторизация составного числа*** | | *2* |
| **Самостоятельная работа обучающихся**  Выполнение индивидуального задания: выполнить шифрование и расшифрование фразы с помощью заданных значений ключа (алгоритм RSA и Эль Гамаля) | | ***4*** |
| **Тема 3.2. Модели криптографических протоколов** | 1 | **Криптографические хеш-функции**   1. [Требования к хэш-функциям](#_Toc245611712). 2. [Простые хэш-функции](#_Toc245611713). 3. [Хэш-функция MD5](#_Toc245611714). 4. [Хэш-функция SHA-1](#_Toc245611715). 5. [Хэш-функции SHA-2](#_Toc245611716). 6. [Хэш-функция ГОСТ Р-34.11](#_Toc245611717)-94 и ГОСТ Р 34.11-2012 Информационная технология. Криптографическая защита информации. Функция хэширования» - российский криптографический стандарт, определяющий алгоритм и процедуру вычисления хеш-функции. | ***4*** | *1* |
| 2 | **Электронная цифровая подпись**   1. Стандарт цифровой подписи. 2. Алгоритм цифровой подписи. 3. ГОСТ Р 34.10-2012 (полное название: «ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи») — российский стандарт, описывающий алгоритмы формирования и проверки электронной цифровой подписи. | *2* | *1* |
| **Практические занятия** | | ***2*** | *2,3* |
| ***Использование программной системы PGP для обеспечения конфиденциальности и целостности информационных ресурсов*** | | *2* |
| **Самостоятельная работа обучающихся**  Выполнение упражнений | | ***4*** |
| **Тема 3.3. Протоколы установления подлинности. Протоколы управления ключами** | 1 | **Программно-аппаратное шифрование**   1. Особенности использования вычислительной техники в криптографии. 2. Различие между программными и аппаратными реализациями. 3. Криптографические параметры узлов и блоков шифраторов. 4. Методы получения случайных и псевдослучайных последовательностей. 5. Вопросы организации сетей засекреченной связи. | ***4*** | *1* |
| **Самостоятельная работа обучающихся**  *Выполнение индивидуального задания*  *Подготовка к зачету* | | ***4*** | *1,2* |
| **Дифференцированный зачет** | | ***1*** |  |
|  | | |  |  |
| **Всего:** | | | ***96*** |  |

Для характеристики уровня освоения учебного материала используются следующие обозначения:

1. – ознакомительный (узнавание ранее изученных объектов, свойств);

2. – репродуктивный (выполнение деятельности по образцу, инструкции или под руководством);

3. – продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач).

# **4. условия реализации программы дисциплины**

**4.1. Требования к минимальному материально-техническому обеспечению**

Реализация программы дисциплины требует наличия лабораторий: компьютерной техники и программно-аппаратных средств защиты информации.

Оборудование: компьютерные классы, оборудованные ПЭВМ из расчета одна ПЭВМ на человека с установленным программным обеспечением: MS Windows, MS Office, Borland Delphi 7, Visual C, комплексы программно-аппаратной криптографической защиты.

Документационное обеспечение: план работы лаборатории, журнал по технике безопасности, интерактивная доска.

Учебно – методическое обеспечение: дидактический материал, учебно- практические пособия по дисциплине, методические рекомендации по организации самостоятельной деятельности студентов, слайд – лекции и презентации по дисциплине, электронные образовательные ресурсы по дисциплине, виртуальный кабинет для самостоятельной работы студентов.

Технические средства обучения: компьютеры с лицензионным программным обеспечением и мультимедиапроектор.

# **4.2. Информационное обеспечение обучения**

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

**Основная**

1. Спирина М.С.,Спирин П.А.Дискретная математика:учебник: Рекомендовано ГОУВПО «МГТУ им. Н. Э. Баумана» для студентов СПО. — 2009, — 368 c.

**Дополнительная**

1. ГОСТ Р 34.311-95 Информационная технология. Криптографическая защита информации. Функция хэширования» - российский криптографический стандарт, определяющий алгоритм и процедуру вычисления хеш-функции.
2. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования данных
3. ГОСТ Р34.10-94. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма
4. ГОСТ Р34.11-94. Информационная технология. Криптографическая защита информации. Функция хэширования
5. ГОСТ Р34.10-2001. Процессы формирования и проверки электронной цифровой подписи
6. ГОСТ Р 34.10-2001. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»)
7. Гашков С., Применко Э., Черепнев М. Криптографические методы защиты информации. – М.: Академия, 2010
8. Хохлов Г.И.Основы теории информации: учебник. — 320 c., 2008 г.

**Internet-ресурсы**

*1) http://www.jetinfo.ru*

*2) www.bezpeka.com*

*3) http://www.criptology.com*

*4) http://*[*www.confident.ru/magazine*](http://www.confident.ru/magazine)

*5)* [*http:/**/www.citforum.ru*](http://www.citforum.ru)

*6)* [*http://www.usp-compulink.ru*](http://www.usp-compulink.ru)

*7)* [*http://www.passwords.ru/*](http://www.passwords.ru/)

*8)* [*http://www.spymarket.com*](http://www.spymarket.com)

*9) www.osp.mesi.ru*

*10) www.nnnn.mesi.ru*

# **5. Контроль и оценка результатов освоения Дисциплины**

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

|  |  |
| --- | --- |
| **Результаты обучения**  **(освоенные умения, усвоенные знания)** | **Формы и методы контроля и оценки результатов обучения** |
| **Усвоенные знания** |  |
| Место и роль криптографических методов в системах защиты государственной, конфиденциальной и коммерческой информации  Требования к шрифтам и основные характеристики шрифтов;  Принципы построения современных шифрсистем;  Основные математические методы, используемые в анализе типовых криптографических алгоритмов  Криптографические протоколы; | Индивидуальный и групповой опрос.  Выполнение практических заданий.  Тестирование.  Выполнение контрольных работ.  Устное собеседование по теоретическому материалу.  Компьютерное тестирование.  Решение ситуационных задач.  Индивидуальная и групповая презентация (представление выполненного задания).  Наблюдение за работой обучающихся.  Подготовка докладов и рефератов.  Дифференцированный зачёт. |
| **Освоенные умения:** |
| Использовать программно-аппаратные средства для обработки шифрованных данных  Рассчитывать параметры типовых шифров замены и перестановки;  Использовать частотные характеристики языков в криптоанализе; |