МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение

инклюзивного высшего образования

«Московский государственный гуманитарно-экономический университет»

Факультет Прикладной математики и информатики

Кафедра Прикладной математики и информатики по областям

|  |  |
| --- | --- |
|  | УТВЕРЖДАЮ |
|  | Проректор по учебной и воспитательной  работе |
|  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  | «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_ г. |

# РАБОЧАЯ ПРОГРАММА

# по ДИСЦИПЛИНе

**«Информационная безопасность»**

образовательная программа направления подготовки

230700.62 «Прикладная информатика»

шифр, наименование

цикл Б.3.Б.08 «Профессиональный цикл,

шифр наименование цикла

Базовая часть

наименование части

Квалификация (степень) выпускника

Бакалавр

Профиль подготовки

Прикладная информатика в менеджменте

Форма обучения очная

Курс 2-3 семестр 4-5

Москва 2014

Рабочая программа составлена на основании федерального государственного образовательного стандарта высшего профессионального образования направления 230700.62 «Прикладная информатика», утвержденного приказом Министерства образования и науки Российской Федерации № 783 от «22» декабря 2009 г. (в редакции приказа Минобрнауки РФ от 31.05.11 №1975). Зарегистрировано в Минюсте России «05» февраля 2010 г. № 16278.

Составители рабочей программы: **\_\_\_\_**МГГЭУ,зав. кафедрой математики**\_\_\_\_\_\_\_**

место работы, занимаемая должность

\_\_\_\_\_\_\_\_\_\_\_\_\_ Терновсков В.Б. 25 августа 2014 г

подпись Ф.И.О. Дата

**Рецензент: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

место работы, занимаемая должность

\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2014 г.

подпись Ф.И.О. Дата

Рабочая программа утверждена на заседании кафедры Прикладной математики и информатики

(протокол № 1 от « 26 » августа 2014 г.)

Заведующий кафедрой \_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2014 г

подпись Ф.И.О. Дата

СОГЛАСОВАНО

Начальник

Учебно-методического управления

«\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_ 2014 г. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_И.Г. Дмитриева \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(дата) (подпись) (Ф.И.О.)

СОГЛАСОВАНО

Декан

факультета

« 30 » августа 2014 г. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Т.В. Заколодина\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(дата) (подпись) (Ф.И.О.)

СОГЛАСОВАНО

Заведующий

библиотекой

«\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_ 2014 г. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(дата) (подпись) (Ф.И.О.)

**1. Цели и задачи дисциплины, ее место в учебном процессе, требования к уровню освоения содержания дисциплины**

**1.1. Цели и задачи изучения дисциплины.**

**Целью** изучения дисциплины является подготовка студентов к освоению организационных, технических, алгоритмических и других методов и средств защиты компьютерной информации, ознакомление с законодательством и стандартами в этой области, с современными криптосистемами, изучение методов идентификации пользователей, борьбы с вирусами, изучение способов применения методов защиты информации при проектировании автоматизированных систем обработки информации и управления (АСОИУ).

**Задачи**:

* определение места дисциплины в предметном блоке, ее взаимосвязи с другими дисциплинами учебного плана специальности;
* раскрытие специфики защиты компьютерных сетей как объекта научного исследования;
* определение основных этапов и базовых концептуальных подходов к созданию систем защиты компьютерных сетей в рамках исторического развития отечественной и зарубежной науки;
* знакомство со способами и особенностями создания систем защиты компьютерных сетей на различных уровнях взаимодействия с окружением;
* приобретение студентами навыков аналитического и эмпирического исследования систем компьютерной защиты сетей;
* выработка целостного представления о различных аспектах строения и функционирования систем компьютерной защиты сетей на всех ее уровнях;
* рост навыков в сфере создания систем компьютерной защиты сетей и умения применять полученные знания на практике.

**1.2. Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля)**

В результате изучения дисциплины студенты должны:

**Знать**:

правовые основы защиты компьютерной информации;

организационные, технические и программные методы защиты информации в АСОИУ;

стандарты, модели и методы шифрования;

методы идентификации пользователей;

методы защиты программ от вирусов и вредоносных программ;

требования к системам информационной защиты АСОИУ и компьютерных сетей.

**Уметь**:

применять методы защиты компьютерных сетей при проектировании АСОИУ в различных предметных областях

**Иметь представление**:

о роли и месте защиты информации в компьютерных сетях;

о направлениях и перспективах развития защиты информации.

***владеть компетенциями:***

|  |  |
| --- | --- |
| **Код**  **компетенции** | **Наименование результата обучения** |
| ОК-1 | способен использовать, обобщать и анализировать информацию, ставить цели и находить пути их достижения в условиях формирования и развития информационного общества |
| ОК-13 | способен понимать сущность и значение информации в развитии современного информационного общества, сознавать опасности и угрозы, возникающие в этом процессе, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны |
| ПК-1 | способен использовать нормативные правовые документы в профессиональной деятельности |
| ПК-8 | способен проводить обследование организаций, выявлять информационные потребности пользователей, формировать требования к информационной системе, участвовать в реинжиниринге прикладных и информационных процессов |
| ПК-13 | способен принимать участие во внедрении, адаптации и настройке прикладных ИС |
| ПК-18 | способен анализировать и выбирать методы и средства обеспечения информационной безопасности |

**1.3. Место дисциплины в структуре ООП**

Учебная программа разрабатывается в тесной взаимосвязи с другими дисциплинами учебного плана специальности, такими как: «Информатика», «Теория распознавания», «Системное и прикладное программное обеспечение», «Методы защиты компьютерных сетей», что предупреждает возможное дублирование учебного материала, обеспечивает целостность изучение предметной области и формирование базового уровня знаний для последующего изучения дисциплин, связанных с данной.

**2. Содержание дисциплины**

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

*Семестр-3,4, вид отчетности: 3 - зачет, 4 - экзамен.*

|  |  |  |  |
| --- | --- | --- | --- |
| № раздела | Наименование  раздела, тема | Содержание раздела | Форма текущего  контроля |
| 1 | 2 | 3 | 4 |
|  | **Радел 1 Основные понятия информационной безопасности и защиты информации.** | Анализ угроз информационной безопасности. Анализ угроз корпоративных сетей. Характерные особенности сетевых атак. Угрозы и уязвимости беспроводных сетей. Тенденции развития ИТ-угроз. Криминализация атак на компьютерные сети и системы. Появление кибероружия для ведения технологических кибервойн. Обеспечение информационной безопасности компьютерных систем. Меры и средства обеспечения информационной безопасности. Пути решения проблем информационной безопасности. | Устный опрос, контрольная работа |
|  | **Раздел 2 Стандарты информационной безопасности.** | Роль стандартов информационной безопасности. Международные стандарты информационной безопасности. Стандарты ISO/IEC 17799:2002 (BS 7799:2000). Германский стандарт BSI. Международный стандарт ISO 15408. «Общие критерии безопасности информационных технологий». Стандарты для беспроводных сетей. Стандарты информационной безопасности для Интернета. Отечественные стандарты безопасности информационных технологий. Стандарт «Критерии оценки безопасности информацион0ных технологий» ГОСТ Р ИСО/МЭК 15408. | Устный опрос контрольная работа |
|  | **Раздел 3 Криптографическая защита информации.** | Основные понятия криптографической защиты информации. Симметричные криптосистемы шифрования. Алгоритмы шифрования DES и 3-DES. Стандарт шифрования ГОСТ 28147-89. Стандарт шифрования AES. Другие симметричные криптоалгоритмы. Основные режимы работы блочного симметричного алгоритма. Особенности применения алгоритмов симметричного шифрования. Асимметричные криптосистемы шифрования. Алгоритм шифрования RSA. Функции хэширования. Электронная цифровая подпись. Отечественный стандарт цифровой подписи ГОСТ Р 34.10-2001. | Устный опрос, контрольная работа |
| **Раздел 4 Принципы многоуровневой защиты корпоративной информации.** | Корпоративная информационная система с традиционной структурой. Системы «облачных» вычислений. Многоуровневый подход к обеспечению информационной безопасности КИС. Безопасность «облачных» вычислений. |
| **Раздел 5 Защита информации в компьютерных сетях, антивирусная защита.** | Концепция построения виртуальных защищенных сетей VPN. PN-решения для построения защищенных сетей. Современные VPN-продукты. |
|  | **Раздел 6 Защита удаленного доступа.** | Особенности удаленного доступа. Средства и протоколы аутентификации удаленных пользователей. Централизованный контроль удаленного доступа. Протокол Kerberos. | Опрос, тестирование, итоговый экзамен |

**3. Структура дисциплины**

|  |  |  |  |
| --- | --- | --- | --- |
| Вид учебной работы | Всего часов | 3 Семестр | 4 Семестр |
| Общая трудоемкость дисциплины | 216 | 108 | 108 |
| *Аудиторные занятия:* | 108 | 54 | 54 |
| Лекции | 44 | 22 | 22 |
| Практические занятия (ПЗ) | 64 | 32 | 32 |
| Семинары (С) |  |  |  |
| Лабораторные работы (ЛР) |  |  |  |
| и(или) другие виды работы |  |  |  |
| *Самостоятельная работа* | 72 | 54 | 18 |
| Курсовой проект (работа) |  |  |  |
| Расчетно-графические работы | 72 | 54 | 18 |
| Реферат и (или) другие виды самостоятельной работы |  |  |  |
| Подготовка и сдача экзамена | 36 | - | 36 |
| Вид итогового контроля |  | Зачет | Экзамен |

**4. Распределение видов учебной работы и их трудоемкости по разделам**

Разделы дисциплины, изучаемые в 3 семестре:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| №  раз-  дела | Наименование разделов | Количество часов | | | | |
| Всего | Аудиторная  работа | | | Внеауд.  работа СР |
| Л | ПЗ | ЛР |
|  | Основные понятия и анализ угроз информационной безопасности | **35** | 7 | 10 | 0 | 18 |
|  | Стандарты информационной безопасности | **35** | 7 | 10 | 0 | 18 |
|  | Криптографическая защита информации | **36** | 8 | 10 | 0 | 18 |
|  | Зачет | **2** |  | 2 |  |  |
|  | *Итого:* | **108** | **22** | **32** | **0** | **54** |

Примечания: 1) Строка «*Всего*» присутствует только в таблице последнего семестра. В ней отражается общее число часов по видам работ за весь период обучения.

Разделы дисциплины, изучаемые в 4 семестре:

| №  Р  аз-  дела | Наименование разделов | | Количество часов | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Всего | Аудиторная  работа | | | Внеауд.  работа СР |
| Л | ПЗ | ЛР |
|  | Принципы многоуровневой защиты корпоративной информации | **23** | | 7 | 10 | 0 | 6 |
|  | Защита информации в компьютерных сетях, антивирусная защита | **23** | | 7 | 10 | 0 | 6 |
|  | Защита удаленного доступа | **26** | | 8 | 12 | **0** | 6 |
|  | *Экзамен* | 36 | |  |  |  |  |
|  | *Итого:* | **108** | | **22** | **32** | **0** | **18** |
|  | *Всего за курс:* |  | | **44** | **64** |  | **72** |

**5. Тематический план учебной дисциплины**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Наименование разделов и тем** | **Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа студентов, курсовая работа (проект)** | | | **Объем часов/**  **зачетных единиц** | **Образовательные технологии** | **Формируемые компетенции/ уровень освоения\*** | **Формы текущего контроля** |
| **1** | **2** | | | **3** | **4** | **5** | **6** |
|  |  | | | **108/3** |  |  |  |
| **1. Основные понятия и анализ угроз информационной безопасности** | **Лекции** | | | 7 | Вводная лекция,  Информационная лекция,  Обзорная лекция | ОК-1,13  ПК-1,8,13,18 | Опрос |
|  | | Анализ угроз информационной безопасности. |
|  | | Характерные особенности сетевых атак. |
|  | | Угрозы и уязвимости беспроводных сетей. |
|  | | Тенденции развития ИТ-угроз. Криминализация атак на компьютерные сети и системы. |
|  | | Появление кибероружия для ведения технологических кибервойн. Обеспечение информационной безопасности компьютерных систем. |
|  | | Меры и средства обеспечения информационной безопасности. |
|  | | Пути решения проблем информационной безопасности. |
| **Практические занятия** | | | 10 | Практическое занятие | ОК-1,13  ПК-1,8,13,18 | Контрольная работа |
|  | | Анализ угроз информационной безопасности. |
|  | | Характерные особенности сетевых атак. |
|  | | Угрозы и уязвимости беспроводных сетей. |
|  | | Тенденции развития ИТ-угроз. Криминализация атак на компьютерные сети и системы. |
|  | | Появление кибероружия для ведения технологических кибервойн. Обеспечение информационной безопасности компьютерных систем. |
|  | | Меры и средства обеспечения информационной безопасности. |
|  | | Пути решения проблем информационной безопасности. |
|  | |  |
| **Самостоятельная работа студента** | | | 18 |  | ОК-1,13  ПК-1,8,13,18 | Контрольная работа |
|  | | Меры и средства обеспечения информационной безопасности. |
| 2 | | Пути решения проблем информационной безопасности. |
| **2. Стандарты информационной безопасности** | **Лекции** | | | 7 | Информационная лекция,  Проблемная лекция,  Лекция-визуализация | ОК-1,13  ПК-1,8,13,18 | Устный опрос |
| 1 | | Роль стандартов информационной безопасности. Международные стандарты информационной безопасности. Стандарты ISO/IEC 17799:2002 (BS 7799:2000). |
|  | **Практические занятия** | | | 10 | Практическое занятие | ОК-1,13  ПК-1,8,13,18 | Контр. работа |
|  | 1 | | Германский стандарт BSI. Международный стандарт ISO 15408. «Общие критерии безопасности информационных технологий». Стандарты для беспроводных сетей. Стандарты информационной безопасности для Интернета. |
|  | **Самостоятельная работа студента** | | | 18 |  |  |  |
| **3. Криптографическая защита информации** | **Лекции** | | | 8 | Проблемная лекция,  Лекция - информация | ОК-1,13  ПК-1,8,13,18 | Опрос |
|  | | Основные понятия криптографической защиты информации. Симметричные криптосистемы шифрования. Алгоритмы шифрования DES и 3-DES. Стандарт шифрования ГОСТ 28147-89. |
|  | | Стандарт шифрования AES. Другие симметричные криптоалгоритмы. Основные режимы работы блочного симметричного алгоритма. Особенности применения алгоритмов симметричного шифрования. |
|  | | Асимметричные криптосистемы шифрования. Алгоритм шифрования RSA. |
|  | | Функции хэширования. |
|  | | Электронная цифровая подпись. Отечественный стандарт цифровой подписи ГОСТ Р 34.10-2001. |
| **Практические занятия** | | | 10 | Практическое занятие | ОК-1,13  ПК-1,8,13,18 | Контрольная работа |
|  | | Стандарт шифрования AES. Другие симметричные криптоалгоритмы. Основные режимы работы блочного симметричного алгоритма. Особенности применения алгоритмов симметричного шифрования. |
|  | | Асимметричные криптосистемы шифрования. Алгоритм шифрования RSA. |
|  | | Электронная цифровая подпись. Отечественный стандарт цифровой подписи ГОСТ Р 34.10-2001. |
| **Самостоятельная работа студента** | | | 18 |  | ОК-1,13  ПК-1,8,13,18 | –– |
| 1 | | Электронная цифровая подпись. Отечественный стандарт цифровой подписи ГОСТ Р 34.10-2001. |
| **4.** Принципы многоуровневой защиты корпоративной информации | **Лекции** | | | 7 | Информационная лекция | ОК-1,13  ПК-1,8,13,18 | Опрос |
|  | | Корпоративная информационная система с традиционной структурой. Системы «облачных» вычислений. |
| 2 | | Многоуровневый подход к обеспечению информационной безопасности КИС. Безопасность «облачных» вычислений |
| **Практические занятия** | | | 10 | Практическое занятие | ОК-1,13  ПК-1,8,13,18 | Устный опрос,  Контрольная работа |
| 1 | | Корпоративная информационная система с традиционной структурой. Системы «облачных» вычислений. |
| 2 | | Многоуровневый подход к обеспечению информационной безопасности КИС. Безопасность «облачных» вычислений |
| **Самостоятельная работа студента** | | | 6 |  | ОК-1,13  ПК-1,8,13,18 | Контрольная работа |
|  | Корпоративная информационная система с традиционной структурой. Системы «облачных» вычислений. | |
| **5.** Защита информации в компьютерных сетях, антивирусная защита защиты корпоративной информации | **Лекции** | | | 7 | Информационная лекция | ОК-1,13  ПК-1,8,13,18 | Опрос |
|  | | Защита информации в компьютерных сетях |
| 2 | | Антивирусная защита. |
| **Практические занятия** | | | 10 | Практическое занятие | ОК-1,13  ПК-1,8,13,18 | Устный опрос,  Контрольная работа |
| 1 | | Защита информации в компьютерных сетях |
| 2 | | Антивирусная защита. |
| **Самостоятельная работа студента** | | | 6 |  | ОК-1,13  ПК-1,8,13,18 | Контрольная работа |
| 6 Защита удаленного доступа | **Лекции** | | | 8 | Информационная лекция | ОК-1,13  ПК-1,8,13,18 | Опрос |
|  | | Особенности удаленного доступа. Средства и протоколы аутентификации удаленных пользователей. |
| 2 | | Централизованный контроль удаленного доступа. Протокол Kerberos**.** |
| **Практические занятия** | | | 12 | Практическое занятие | ОК-1,13  ПК-1,8,13,18 | Устный опрос,  Контрольная работа |
| 1 | | Особенности удаленного доступа. Средства и протоколы аутентификации удаленных пользователей. |
| 2 | | Централизованный контроль удаленного доступа. Протокол Kerberos**.** |
| **Самостоятельная работа студента** | | | 6 |  |  | Контрольная работа |

\* В таблице уровень усвоения учебного материала обозначен цифрами:

1. – репродуктивный (освоение знаний, выполнение деятельности по образцу, инструкции или под руководством);

2.  – продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач; применение умений в новых условиях);

3. – творческий (самостоятельное проектирование экспериментальной деятельности; оценка и самооценка инновационной деятельности).

**6. Образовательные технологии**

*Проблемные технологии обучения.*

Интерактивные лекции-диалоги. Лекции в условиях активного использования информационных технологий становятся более динамичными и обладают большим коэффициентом диалога и активного использования демонстрационных материалов.

Компьютерные технологии обучения и тестирования. Значительную роль при организации обучения на основе любой образовательной технологии имеет контроль полученного уровня знаний и практических умений.

Технологии контекстного обучения. Применение контекстного обучения значительно сокращает дельта времени между непониманием вопроса из-за неполноты сведений по предыдущим вопросам или недостаточного уровня подготовленности студентов по конкретному вопросу.

Сетевые информационные интернет-технологии обучения и взаимодействия. Важный компонент организации лабораторной и самостоятельной работы обучающихся, способствует развитию навыков самообразования, формированию информационной и поисковой культуры, новых соответствующих компетенций у обучающихся. Являются основой дистанционно-образовательных технологий обучения.

Личностно-деятельностные технологии обучения − психолого-педагогическая и технологическая основа организации лабораторной и самостоятельной работы обучающихся, способствует развитию навыков самообразования, формированию информационной и поисковой культуры, новых соответствующих компетенций обучающихся.

**Интерактивные образовательные технологии, используемые в аудиторных занятиях**

|  |  |  |  |
| --- | --- | --- | --- |
| **Семестр** | **Вид занятия**  **(Л, ПР, ЛР)** | **Используемые интерактивные образовательные технологии** | **Количество**  **часов** |
| 3 | Л | Коммуникативная лекция, презентации с использованием интерактивных досок | 10 |
| ПР | Ролевое построение семинара - докладчик и оппоненты (100%)  Компьютерное тестирование (MyTest) | 12 |
| ЛР | - |  |
| **Итого:** | | | 22 |

1. Для обучения учащихся, имеющих ограниченные физические возможности, качественного образования должны выполняться следующие важные условия: учащийся должен иметь возможность беспрепятственно посещать образовательное учреждение и использовать в своём обучении дистанционные образовательные технологии. (реализовано на базе системы Moodle)
2. Для беспрепятственного прохода в здание людей с ограниченными физическими возможностями учреждение располагает пандусом; для обеспечения беспрепятственного прохода в аудитории инвалидов-колясочников парты и стулья должны быть расставлены без нагромождений. (компьютерные аудитории 401, 402, 308, 2-120) Для обучения и контроля учащихся с нарушениями координации движений предусмотрено проведение тестирования с использованием компьютера. (реализовано в программе MyTest)

**7. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации**

**7.1.Организация входного, текущего и промежуточного контроля обучения**

**7.2. Организация контроля:**

* **(пример)** Входное тестирование – контрольный тест
* Текущий контроль – опрос
* Промежуточная аттестация – контрольные работы

**7.3. Тематика рефератов, проектов, творческих заданий, эссе и т.п. – нет.**

**7.4. Курсовая работа - не предусмотрена**

**7.5. Вопросы к зачету**

1. Уточнение задач информационной безопасности организации. Изучение источников, рисков и форм атак на информацию в АСОИУ.
2. Изучение источников, рисков и форм атак на информацию в АСОИУ. Классификация рисков и основные задачи обеспечения безопасности информации в АСОИУ.
3. Изучение Российского законодательства по защите информационных технологий. Изучение нормативно-правовой информации, определяющей функционирование систем защиты. Разработка политики информационной безопасности организации.
4. Изучение международных и Государственных стандартов информационной безопасности.
5. Изучение симметричных и ассиметричных криптосистем для защиты компьютерной информации в АСОИУ.
6. Изучение стандартных алгоритмов шифрования. Безопасность и быстродействие криптосистем.
7. Изучение принципов идентификации и механизмов подтверждения подлинности пользователя. Правила формирования электронной цифровой подписи.
8. Изучение средств защиты локальных сетей от несанкционированного доступа. Анализ функционирования маршрутизаторов, шлюзов сетевого уровня и межсетевых экранов.
9. Анализ способов защиты информации в компьютерных сетях от разрушающего программного воздействия. Изучение методов борьбы с компьютерными вирусами и средств защиты информации в Internet. Угрозы исходящие от использования «электронной почты».
10. Изучение требований по обеспечению информационной безопасности к аппаратным средствам и программному обеспечению АСОИ. Порядок и правила организации аудита информационной безопасности АСОИУ и предприятия в целом.
11. Понятие информационной безопасности. Характеристики информации с позиции безопасности.
12. Классификация угроз безопасности информации.
13. Классификация угроз безопасности распределенных вычислительных систем
14. Модель OSI.
15. Объясните понятие «политика безопасности организации».
16. Какие разделы должна содержать документально оформленная политика безопасности?
17. Какие проблемы решает верхний уровень политики безопасности?
18. Какие задачи решает средний уровень политики безопасности?
19. Каковы особенности нижнего уровня политики безопасности?
20. Сформулируйте главную задачу стандартов информационной безопасности с позиций производителей и потребителей продуктов информационных технологий, а также специалистов по сертификации этих продуктов.
21. Назовите основные международные стандарты информационной безопасности.
22. Дайте краткую характеристику международного стандарта 17799 (BS 7799).
23. Каковы основные особенности германского стандарта BSI «Руководство по защите информационных технологий для базового уровня защищенности».
24. Перечислитe стандарты для беспроводных сетей и дайте их краткую характеристику.
25. Назовите стандарты информационной безопасности для Internet.

**Вопросы к экзамену**

1. Каковы назначение и особенности функционирования протокола SET.
2. Каковы назначение и функциональность протоколов SSL и IPSec.
3. Каково назначение стандарта ГОСТ Р ИСО/МЭК 15408. Назовите и охарактеризуйте три основные части этого стандарта.
4. Обобщенная схема криптосистемы шифрования
5. Классификация криптографических алгоритмов
6. Схема симметричной криптосистемы шифрования
7. Алгоритм шифрования DES и 3DES
8. Стандарт шифрования ГОСТ 28147-89
9. Стандарт шифрования AES
10. Режимы работы блочного симметричного алгоритма
11. Дайте определение однонаправленной функции. Каковы особенности однонаправленных функции.
12. Опишите две основные процедуры, осуществляемые системой электронной цифровой подписи для подтверждения подлинности электронного документа.
13. Каково назначение хэш-функции и каким требованиям должна удовлетво­рять качественная хэш-функция?
14. Дать определение понятия «идентификация», «аутентификация», «авторизация», «администрирование».
15. На какие категории можно разделить процессы аутентификации в зави­симости от сущностей, предъявляемых пользователем для подтверждения своей подлинности?
16. Опишите метод аутентификации на основе мно призовых паролей. Каковы его недостатки?
17. Опишите метод аутентификации на основе одноразовых паролей. Каковы его достоинства и недостатки?
18. Сформулируйте принцип строгой аутентификации.
19. Объясните назначение PIN-кода и особенности его использования.
20. Объясните принцип работы двухфакторной аутентификации. Какие вне­шние носители информации используют для двухфакторной аутентифи­кации пользователей? Каковы достоинства этого метода аутентификации?
21. Опишите функциональность и характеристики смарт-карт и USB-токенов.
22. Опишите методы биометрической аутентификации пользователя.
23. Объясните принцип управления доступом по схеме однократного входа с авторизацией SSO.

**7.6 Критерии оценки**

***Критерии оценки зачета***

* Проведение зачетов предусматривает: подведение итогов по всему учебному курсу или отдельным наиболее важным его разделам, выявление степени усвоения студентами изученного материала, наличие навыков самостоятельной работы по изучению учебной и научной литературы.
* Результаты сдачи зачетов определяются двумя оценками - «зачтено» или «не зачтено». Они могут оцениваться по пятибалльной системе, если предусмотрен дифференцированный зачёт.
* Оценка «**зачтено**» предполагает знание структуры курса, темы, излагаемого вопроса, основной литературы, способность сделать самостоятельные выводы, умение выделить главное, комментировать излагаемый материал. Возможны несущественные пробелы в усвоении некоторых вопросов.
* Оценка «**Не зачтено**» ставится в случае, когда студент не знает значительной части
* учебного материала, допускает существенные ошибки, когда знания носят отрывочный и бессистемный характер, нет понимания важных, узловых вопросов курса, а на большинство дополнительных вопросов даны ошибочные ответы.

**Критерии оценки экзамена**

* оценка **«отлично»** выставляется студенту, если он глубоко и прочно усвоил программный материал курса, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами и вопросами, причем не затрудняется с ответами при видоизменении заданий, правильно обосновывает принятые решения, владеет разносторонними навыками и приемами выполнения практических задач;
* оценка **«хорошо»** выставляется студенту, если он твердо знает материал курса, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения;
* оценка «**удовлетворительно»** выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических задач;
* оценка **«неудовлетворительно»** выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями решает практические задачи или не справляется с ними самостоятельно.

**7.6 Тематика рефератов (курсовых работ)**

не предусмотрено

1. **Сведения о материально-техническом обеспечении дисциплины**

|  |  |  |
| --- | --- | --- |
| №  п/п | Наименование оборудованных учебных кабинетов, лабораторий | Перечень оборудования и технических средств обучения |
| 1 | Лекционная аудитория | Мультимедиа-проектор |
| 2 | Компьютерный класс | - |

**9. Учебно-методическое обеспечение дисциплины**

**9.1. Основная литература**

1. Бабаш А.В. Информационная безопасность. Лабораторный практикум (+CD) : учеб.пособие / Бабаш, Александр Владимирович , Баранова, Елена Константиновна , Мельников, Юрий Николаевич . - 2-е изд., стереотип. ; CD-диск. - М. : Эком, 2013. - 136с.: ил. + библ. – (Бакалавриат). – ISBN 978-5-406-02760-8
2. Маркеев, Александр Иванович. Правовая защита информации : учеб.пособие для вузов / Сибирск.гос.геодезич.акад. - Новосибирск : УМЦ ВПО, 2011. - 179с. + библ.

**9.2. Дополнительная** **литература**

1. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си – М.: «Триумф», 2010.
2. Информационная безопасность компьютерных систем и сетей : учеб. пособие для средн. проф. образования по спец. "Информатика и ВТ" / Шаньгин, Владимир Федорович. - М. : Форум, 2010 ; : Инфра-М. - 416с. - (Профессиональное образование). - ISBN 978-5-8199-0331-5. - ISBN 978-5-16-003132-3 : 115.39.
3. Информационное право : учеб. для юридич. спец. вузов / Городов, Олег Александрович. - М. : Проспект, 2011. - 248с. - ISBN 978-5-482-01373-1 : 109.23.
4. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. Учебное пособие. – М.: «Гелиос АРВ», 2011.
5. Чмора А.Л. Современная прикладная криптография. – М.: «Гелиос АРВ», 2010.
6. Введение в криптографию / Под общ. ред. В.В. Ященко. – 3-е изд., доп. – М.: МЦНМО, «ЧеРо», 2009.
7. Столингс В. Криптография и защита сетей. Принципы и практика. 2-е изд. – М.: Издательский дом «Вильямс», 2011.

**9.3. Учебно-методическое и информационное обеспечение дисциплины для организации самостоятельной работы студентов** (содержит перечень основной литературы, дополнительной литературы, программного обеспечения и Интернет-ресурсы)

1. <http://kiev-security.org.ua/box/2/26.shtml>
2. <http://asu.gubkin.ru/> - Методы и средства защиты информации
3. [http://www.osp.ru/ - Журнал «Открытые Системы](http://www.osp.ru/os/os_1_96/os.htm)»
4. [http://www.compulog.ru/](http://www.compulog.ru/hackzone/index.html) - [Журнал «HackZone](http://www.compulog.ru/hackzone/index.html)»
5. <http://www.iso.org/> Международные стандарты безопасности ISO
6. <http://www.citforum.ru/>
7. <http://www.groteck.ru/security_ru> - Журнал «Информационная безопасность»
8. [http://securitylab.ru/](http://securitylab.ru/?id=31853)
9. [http://www.networkdoc.ru/](http://www.networkdoc.ru/index.html)
10. <http://cryptography.ru/>