МИНОБРНАУКИ РОССИИ
**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**
**«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»**
**(ФГБОУ ВО «ВГУ»)**

УТВЕРЖДАЮ
Заведующий кафедрой
математического анализа
_____А.Д. Баев
30.05.2019г.

# РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

## Б1.Б.33 Безопасность информационных и аналитических систем

**1. Код и наименование направления подготовки/специальности:**
10.05.04 Информационно-аналитические системы безопасности

**2. Профиль подготовки/специализация:** Информационная безопасность финансовых и экономических структур

**3. Квалификация выпускника:** специалист по защите информации

**4. Форма обучения:** очная

**5. Кафедра, отвечающая за реализацию дисциплины:** математического анализа

**6. Составители программы:**
Найдюк Филипп Олегович, канд. физ.-мат. наук, доцент кафедры математического анализа

**7**. **Рекомендована:** Научно-методическим Советом математического факультета, протокол от № 0500-05 от 27.05.2019 г.

**8. Учебный год:** 2022/2023 **Семестр(ы):** 7

**9. Цели и задачи учебной дисциплины:**

В результате изучения дисциплины «Безопасность информационных и аналитических систем» обучающийся должен:

*знать:*
- сущность и понятие информации, информационной безопасности и характеристику ее составляющих;
- источники и классификацию угроз информационной безопасности;
- основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации;
- основные виды и угрозы безопасности операционных систем;
- основные стандарты в области инфокоммуникационных систем и технологий;
- защитные механизмы и средства обеспечения сетевой безопасности;
- средства и методы предотвращения и обнаружения вторжений;
- основные отечественные и зарубежные стандарты в области компьютерной безопасности;
- основные методы организационного обеспечения информационной безопасности специальных АИС;
- логико-лингвистические основы обработки данных и знаний в специальных АИС;
- системы распределенной обработки данных, используемые в специальных АИС;
- нормативную базу, регламентирующую создание и эксплуатацию специальных АИС;
- назначение и классификацию информационных и аналитических систем, систем управления;
- принципы эксплуатации и сопровождения АИС;

*уметь:*
- классифицировать и оценивать угрозы информационной безопасности для объекта информатизации;
- использовать модели данных и знаний для решения стандартных задач автоматизации;
- решать задачи исследования специальных АИС методами моделирования;
- применять языковые, программные и аппаратные средства исследования эффективности технологических процессов обработки информации в специальных АИС;
- применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях;
- осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты;
- пользоваться средствами защиты, предоставляемыми системами управления базами данных;
- применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем;

*владеть:*
- навыками безопасного использования технических средств в профессиональной деятельности;
- навыками моделирования технологических процессов обработки информации в специальных АИС с заданной степенью статистической надежности результатов;

- навыками исследования математических моделей технологических процессов обработки информации в специальных АИС с целью оценки качества и оптимизации характеристик специальных АИС;
- методами и средствами выявления угроз безопасности компьютерным системам;
- методами моделирования безопасности компьютерных систем, в том числе, моделирования управления доступом и информационными потоками в компьютерных системах;
- основами маршрутизации и управления потоками в сетях передачи информации.

**10. Место учебной дисциплины в структуре ООП:**

Дисциплина «Безопасность информационных и аналитических систем» относится к учебным дисциплинам базовой части блока Б1 основной образовательной программы по направлению 10.05.04 «Информационно-аналитические системы безопасности».

Дисциплина «Безопасность информационных и аналитических систем» базируется на знаниях, полученных по дискретной математике, информатике, численным методам и методам оптимизации.

Приобретенные в результате обучения знания, умения и навыки используются в рамках последующих предметов:

- принципы построения, проектирования и эксплуатации автоматизированных информационных систем;
- управление информационной безопасностью.

**11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями выпускников):**

| Компетенция | | Планируемые результаты обучения |
|---|---|---|
| Код | Название | |
| ОПК-7 | способность применять методы и средства обеспечения информационной безопасности специальных ИАС | знать:<br>- сущность и понятие информации, информационной безопасности и характеристику ее составляющих;<br>- источники и классификацию угроз информационной безопасности; основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации;<br>- средства и методы предотвращения и обнаружения вторжений;<br>- основные отечественные и зарубежные стандарты в области компьютерной безопасности;<br>- основные методы организационного обеспечения информационной безопасности специальных АИС; - назначение и классификацию информационных и аналитических систем, систем управления<br><br>уметь:<br>- классифицировать и оценивать угрозы |

| | | |
|---|---|---|
| | | информационной безопасности для объекта информатизации; пользоваться средствами защиты, предоставляемыми системами управления базами данных;<br>- применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем<br><br>владеть:<br>- навыками моделирования технологических процессов обработки информации в специальных АИС с заданной степенью статистической надежности результатов;<br>- навыками исследования математических моделей технологических процессов обработки информации в специальных АИС с целью оценки качества и оптимизации характеристик специальных АИС |
| ПК-3 | способность осуществлять сбор, изучение, анализ и обобщение научно-технической информации, нормативных и методических материалов в области технологий информационно-аналитической деятельности и специальных ИАС, в том числе средств обеспечения их информационной безопасности | знать:<br>- источники и классификацию угроз информационной безопасности;<br>- основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации;<br>- основные виды и угрозы безопасности операционных систем;<br>- основные стандарты в области инфокоммуникационных систем и технологий;<br>- защитные механизмы и средства обеспечения сетевой безопасности;<br>- средства и методы предотвращения и обнаружения вторжений;<br>- основные отечественные и зарубежные стандарты в области компьютерной безопасности;<br>- основные методы организационного обеспечения информационной безопасности специальных АИС<br><br>уметь:<br>- классифицировать и оценивать угрозы информационной безопасности для объекта информатизации; решать задачи исследования специальных АИС методами моделирования;<br>- применять языковые, программные и аппаратные средства исследования эффективности технологических процессов обработки информации в специальных АИС;<br>- решать задачи построения и эксплуатации распределенных автоматизированных систем обработки данных |

| | | |
|---|---|---|
| | | владеть:<br>- навыками безопасного использования технических средств в профессиональной деятельности |
| ПК-9 | способность выявлять основные угрозы безопасности информации, строить и исследовать модели нарушителя в компьютерных системах | знать:<br>- основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации; защитные механизмы и средства обеспечения сетевой безопасности;<br>- средства и методы предотвращения и обнаружения вторжений;<br><br>уметь:<br>- классифицировать и оценивать угрозы информационной безопасности для объекта информатизации; применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях;<br>- осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты;<br>- пользоваться средствами защиты, предоставляемыми системами управления базами данных;<br>- применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем<br><br>владеть:<br>- методами и средствами выявления угроз безопасности компьютерным системам;<br>- методами моделирования безопасности компьютерных систем, в том числе, моделирования управления доступом и информационными потоками в компьютерных системах;<br>- простейшими методами анализа безопасности криптографических протоколов |
| ПК-10 | способность осуществлять выбор технологии, инструментальных средств, средств вычислительной техники и средств обеспечения информационной | знать:<br>- назначение и классификацию информационных и аналитических систем, систем управления;<br>- принципы эксплуатации и сопровождения АИС;<br>- основные методы организационного обеспечения информационной безопасности специальных АИС |

| | | |
|---|---|---|
| | безопасности создаваемых специальных ИАС | уметь:<br>- применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем<br><br>владеть:<br>- навыками анализа и синтеза структурных и функциональных схем технологических процессов обработки информации в специальных АИС;<br>- навыками выбора и обоснования критериев эффективности функционирования специальных АИС |
| ПК-13 | способность оценивать эффективность специальных ИАС, в том числе средств обеспечения их информационной безопасности | знать:<br>- методологические основы, методы и средства моделирования специальных АИС;<br>- методы построения и исследования математических моделей специальных АИС;<br>- методы планирования и оптимизации компьютерных экспериментов с моделями специальных АИС;<br>- методологические основы, методы и средства построения распределенных специальных АИС;<br>- системы распределенной обработки данных, используемые в специальных АИС;<br>нормативную базу, регламентирующую создание и эксплуатацию специальных АИС<br><br>уметь:<br>- проектировать и сопровождать типовые специальные АИС, локальные сети;<br>- осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты;<br>- пользоваться средствами защиты, предоставляемыми системами управления базами данных<br><br>владеть:<br>- навыками анализа программных реализаций;<br>- методами моделирования безопасности компьютерных систем, в том числе, моделирования управления доступом и информационными потоками в компьютерных системах |

**12. Объем дисциплины в зачетных единицах/часах в соответствии с учебным планом —** 3/108.

**Форма промежуточной аттестации** зачёт с оценкой.

**13. Виды учебной работы:**

| Вид учебной работы | Трудоемкость (часы) | | | | |
|---|---|---|---|---|---|
| | Всего | По семестрам | | | |
| | | 7 сем. | 8 сем. | 9 сем. | 10 сем. |
| Аудиторные занятия | 50 | 50 | | | |
| в том числе: лекции | 16 | 16 | | | |
| практические | | | | | |
| лабораторные | 34 | 34 | | | |
| СРС | 58 | 58 | | | |
| Контроль | | | | | |
| Итого: | 108 | 108 | | | |

**13.1 Содержание разделов дисциплины:**

| № п/п | Наименование раздела дисциплины | Содержание раздела дисциплины |
|---|---|---|
| Лекции | | |
| 1.1 | Понятия информационной безопасности (ИБ). Ключевые вопросы ИБ. | Исторические моменты формирования ИБ. Составляющие информационной безопасности. Доктрина информационной безопасности РФ. Общая структура ИБ. Требования по обеспечению ИБ. Классификация защиты информации. Ранжирование ИТ-угрозы. Спецификация полей ИБ. |
| 1.2 | Виды угроз ИБ и методы их анализа. | Критерии классификации угроз ИБ. Модели. Алгоритмы анализа угрозы и оценки ИБ. Основные виды защищаемой информации. |
| 1.3 | Правовое обеспечение ИБ | Российское законодательство в области ИБ: законы, постановления и другие нормативные акты. |
| 1.4 | Построение системы ИБ | Уровни программы информационной безопасности. Математические модели в реализации концепции и программы ИБ. Системы защиты информации (СЗИ). Генетический алгоритм. Анализ и управление рисками при реализации ИБ. Защита информации в информационных системах и компьютерных сетях. |
| 1.5 | Информационные системы (ИС) и обеспечение их безопасности | Трёхуровневая модель оценки защищённости ИС. Требования к архитектуре ИС. Стандарты. Технологии криптографической защиты информации. Межсетевые экраны. Защищённые виртуальные сети VPN. Антивирусная защита. Классификация угроз ИС: сетевые черви, вирусы, |

| | | |
|---|---|---|
| | | троянские программы и прочие вредоносные утилиты. |
| 1.6 | Создание архитектуры информационно-аналитических систем (ИАС) | Аналитические системы: процессы и инструменты. Описание общей структуры. Степени ИБ. Особенности применения и анализа информации. |
| Лабораторные работы | | |
| 2.1 | Методы анализа угроз ИБ | Алгоритмы анализа угрозы и оценки ИБ. Классификация основных видов защищаемой информации. |
| 2.2 | Построение системы ИБ | Математические модели в реализации концепции и программы ИБ. Использование систем защиты информации (СЗИ). Генетический алгоритм. Построение защиты информации в информационных системах и компьютерных сетях. |
| 2.3 | Информационные системы (ИС) и обеспечение их безопасности | Создание и анализ трёхуровневой модели оценки защищённости ИС. Эксплуатация межсетевых экранов. Технологии криптографической защиты информации. Оценка защищённости виртуальных сетей VPN. Антивирусная защита. Классификация угроз ИС |
| 2.4 | Создание архитектуры ИАС | Использование аналитических систем. Создание общей структуры по степеням ИБ |

**13.2. Темы (разделы) дисциплины и виды занятий:**

| № п/п | Наименование раздела дисциплины | Виды занятий (часов) | | | | |
|---|---|---|---|---|---|---|
| | | Лекции | Практические | Лабораторные | СРС | Всего |
| 01 | Понятия информационной безопасности (ИБ). Ключевые вопросы ИБ. | 1 | | 1 | 2 | 4 |
| 02 | Виды угроз ИБ и методы их анализа. | 2 | | 1 | 10 | 13 |
| 03 | Правовое обеспечение ИБ | 1 | | | 11 | 12 |
| 04 | Построение системы ИБ | 4 | | 12 | 11 | 27 |
| 05 | Информационные системы (ИС) и обеспечение их безопасности. | 4 | | 10 | 11 | 25 |
| 06 | Создание архитектуры информационно-аналитических систем (ИАС) | 4 | | 12 | 13 | 29 |
| Итого | | 16 | | 34 | 58 | 108 |

**14. Методические указания для обучающихся по освоению дисциплины:**

В процессе освоения дисциплины студенты должны посетить лекционные и лабораторные занятия и сдать зачёт на оценку.

Указания для освоения теоретического и практического материала и сдачи зачёта:

1. Обязательное посещение лекционных и лабораторных занятий по дисциплине с конспектированием излагаемого преподавателем материала в соответствии с расписанием занятий.

2. Получение в библиотеке рекомендованной учебной литературы и электронное копирование рабочей программы с методическими рекомендациями, конспекта лекций.

3. Копирование (электронное) перечня вопросов к экзамену по дисциплине, а также списка рекомендованной литературы из рабочей программы дисциплины.

4. При подготовке к лабораторным занятиям по дисциплине необходимо изучить рекомендованный лектором материал, иметь при себе конспекты соответствующих тем и необходимый справочный материал.

5. Рекомендуется следовать советам лектора, связанным с освоением предлагаемого материала, провести самостоятельный Интернет – поиск информации (видеофайлов, файлов-презентаций, файлов с учебными пособиями) по ключевым словам курса и ознакомиться с найденной информацией при подготовке к зачёту по дисциплине.

Студент допускается к сдаче зачёта, если имеет на руках конспект основного теоретического материала с разбором основных типовых задач, имеется зачёт по контрольной работе.

## 15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины:

а) основная литература:

| № п/п | Источник |
|---|---|
| 1 | ***Голуб, В. А**. Информационная безопасность компьютерных систем. Защита целостности информации / В.А. Голуб.– Воронеж: ЛОП ВГУ, 2006.– 31 с.* |
| 2 | ***Смирнов, С. Н**. Безопасность систем баз данных / С.Н. Смирнов.– М.: Гелиос АРВ, 2007.– 350 с.* |
| 3 | ***Астанин, И. К**. Защита информации / И.К. Астанин, Н.И. Астанин.– Воронеж: Воронеж. гос. ун-т, 2006.– с.169* |
| 4 | ***Мельников, В. П**. Информационная безопасность и защита информации / В.П. Мельников, С.А. Клейменов, А.М. Петраков.– М.: ACADEMIA, 2006.– 330 с.* |

б) дополнительная литература:

| № п/п | Источник |
|---|---|
| 5 | ***Галицкий, А. В**. Защита информации в сети - анализ технологий и синтез решений / А.В. Галицкий, С.Д. Рябко, В.Ф. Шаньгин.– М.: ДМК Пресс, 2004.– 613 с.* |
| 6 | ***Завгородний, В. И**. Комплексная защита информации в компьютерных системах: Учебное пособие для студ. вузов / В.И. Завгородний.– М.: Логос, 2001.– 262 с.* |
| 7 | ***Гайдамакин, Н. А**. Автоматизированные информационные системы, базы и банки данных / Н.А. Гайдамакин.– М.: Гелиос АРВ, 2002.– 367 с.* |
| 8 | ***Мизин, И.А.** Автоматизированные системы управления. Основы теории информационных систем / И.А. Мизин, Л.С. Уринсон, Г.К. Храмешин;* |

| | |
|---|---|
| | *Московский институт радиотехники, электроники и автоматики.– М., 1971.– 173 с.* |
| 9 | ***Ярочкин, В. И.*** *Безопасность информационных систем / В. И. Ярочкин.– М.: Ось-89, 1996.– 318 с.* |
| 10 | ***Круглов, В. В****. Интеллектуальные информационные системы: Компьютерная поддержка систем нечеткой логики и нечеткого вывода / В.В. Круглов, М.И. Дли.– М.: Физматлит, 2002.– 254 с.* |

в) информационные электронно-образовательные ресурсы**:**

| № п/п | Источник |
|---|---|
| 11 | *Электронный каталог Научной библиотеки Воронежского государственного университета. – (http // www.lib.vsu.ru/)* |
| 12 | *Официальный сайт компании «BaseGroup Labs» [Электрон. ресурс]. Рязань, 1995-2010.- Режим доступа: http://www.basegroup.ru/* |
| 13 | *Электронно-библиотечная система "Консультант студента". – (http://www.studentlibrary.ru/)* |
| 14 | *Электронно-библиотечная система «Издательства Лань». – (https://e.lanbook.com/)* |
| 15 | *Электронно-библиотечная система "РУКОНТ". – (https://rucont.ru/)* |

**16. Перечень учебно-методического обеспечения для самостоятельной работы:**

Курс дисциплины построен таким образом, чтобы позволить студентам проявить способность к самостоятельной работе. Для успешной самостоятельной работы предполагается интерактивный диалог с преподавателем, осуществляемый с помощью удаленной связи через интернет.

Самостоятельная работа студента, прежде всего, заключатся в изучении литературы, дополняющей материал, излагаемый на лекции и в ходе лабораторных работ. Необходимо овладеть навыками библиографического поиска, уметь находить подходящие источники, творчески и критически перерабатывать информацию, научиться определять методы исследований.

**17. Информационные технологии, используемые для реализации учебной дисциплины, включая программное обеспечение и информационно-справочные системы (при необходимости)**

Осуществляется интерактивная связь с преподавателем через сеть интернет, проводятся индивидуальные онлайн консультации и проверка контрольных работ.

Лабораторные работы осуществляются с использованием ЭВМ и прикладного ПО: Deductor.

**18. Материально-техническое обеспечение дисциплины:**

Учебные аудитории для проведения лекционных и практических занятий. Компьютерные классы для выполнения индивидуальных заданий, оснащённые лицензионным и свободно распространяемым программным обеспечением: Windows 7 или 10, информационно-аналитическая платформа Deductor, Wireshark.

**19. Фонд оценочных средств:**

**19.1. Перечень компетенций с указанием этапов формирования и планируемых результатов обучения**

| Код и содержание компетенции | Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенции посредством формирования знаний, умений, навыков) | Этапы формирования компетенции (разделы (темы) дисциплины или модуля и их наименование) | ФОС |
|---|---|---|---|
| ОПК-7: способность применять методы и средства обеспечения информационной безопасности специальных ИАС | знать:<br>- сущность и понятие информации, информационной безопасности и характеристику ее составляющих;<br>- источники и классификацию угроз информационной безопасности;<br>- основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации;<br>- средства и методы предотвращения и обнаружения вторжений;<br>- основные отечественные и зарубежные стандарты в области компьютерной безопасности;<br>- основные методы организационного обеспечения информационной безопасности специальных АИС;<br>- назначение и классификацию информационных и аналитических систем, систем управления | 01, Понятия информационной безопасности (ИБ); 02, Виды угроз ИБ и методы их анализа; 03, Правовое обеспечение ИБ; 04, Построение системы ИБ | Устный опрос |
| | уметь:<br>- классифицировать и оценивать угрозы информационной | 04, Построение системы ИБ; 05, Информационные системы (ИС) и | Устный опрос |

| | | | |
|---|---|---|---|
| | безопасности для объекта информатизации;<br>- пользоваться средствами защиты, предоставляемыми системами управления базами данных;<br>- применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем | обеспечение их безопасности; 06, Создание архитектуры информационно-аналитических систем (ИАС) | |
| | владеть:<br>- навыками моделирования технологических процессов обработки информации в специальных АИС с заданной степенью статистической надежности результатов;<br>- навыками исследования математических моделей технологических процессов обработки информации в специальных АИС с целью оценки качества и оптимизации характеристик специальных АИС | 04, Построение системы ИБ; 05, Информационные системы (ИС) и обеспечение их безопасности; 06, Создание архитектуры информационно-аналитических систем (ИАС) | Практическое задание |
| ПК-3: способность осуществлять сбор, изучение, анализ и обобщение научно-технической информации, нормативных и методических материалов в области технологий информационно-аналитической | знать:<br>- источники и классификацию угроз информационной безопасности;<br>- основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации;<br>- основные виды и угрозы безопасности операционных систем;<br>- основные стандарты в | 01, Понятия информационной безопасности (ИБ); 02, Виды угроз ИБ и методы их анализа; 03, Правовое обеспечение ИБ; 06, Создание архитектуры информационно-аналитических систем (ИАС) | Устный опрос |

| | | | |
|---|---|---|---|
| деятельности и специальных ИАС, в том числе средств обеспечения их информационной безопасности | области инфокоммуникационных систем и технологий;<br>- защитные механизмы и средства обеспечения сетевой безопасности;<br>- средства и методы предотвращения и обнаружения вторжений;<br>- основные отечественные и зарубежные стандарты в области компьютерной безопасности;<br>- основные методы организационного обеспечения информационной безопасности специальных АИС | | |
| | уметь:<br>- классифицировать и оценивать угрозы информационной безопасности для объекта информатизации; решать задачи исследования специальных АИС методами моделирования;<br>- применять языковые, программные и аппаратные средства исследования эффективности технологических процессов обработки информации в специальных АИС;<br>- решать задачи построения и эксплуатации распределенных автоматизированных систем обработки данных | 01, Понятия информационной безопасности (ИБ); 02, Виды угроз ИБ и методы их анализа; 04, Построение системы ИБ; 05, Информационные системы (ИС) и обеспечение их безопасности | Устный опрос |
| | владеть:<br>- навыками безопасного использования технических средств в профессиональной деятельности | Виды угроз ИБ и методы их анализа; 03, Правовое обеспечение ИБ; 04, Построение системы ИБ; 06, | Практическое задание |

| | | | |
|---|---|---|---|
| | | Создание архитектуры информационно-аналитических систем (ИАС) | |
| ПК-9: способность выявлять основные угрозы безопасности информации, строить и исследовать модели нарушителя в компьютерных системах | знать: - основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации;<br>- защитные механизмы и средства обеспечения сетевой безопасности;<br>- средства и методы предотвращения и обнаружения вторжений | 02, Виды угроз ИБ и методы их анализа | Устный опрос |
| | уметь:<br>- классифицировать и оценивать угрозы информационной безопасности для объекта информатизации;<br>- применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях;<br>- осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты;<br>- пользоваться средствами защиты, предоставляемыми системами управления базами данных;<br>- применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности | 02, Виды угроз ИБ и методы их анализа | Устный опрос |

| | | | |
|---|---|---|---|
| | компьютерных систем | | |
| | владеть:<br>- методами и средствами выявления угроз безопасности компьютерным системам;<br>- методами моделирования безопасности компьютерных систем, в том числе, моделирования управления доступом и информационными потоками в компьютерных системах;<br>- простейшими методами анализа безопасности криптографических протоколов | 02, Виды угроз ИБ и методы их анализа | Практическое задание |
| ПК-10: способность осуществлять выбор технологии, инструментальных средств, средств вычислительной техники и средств обеспечения информационной безопасности создаваемых специальных ИАС | знать:<br>- назначение и классификацию информационных и аналитических систем, систем управления;<br>- принципы эксплуатации и сопровождения АИС;<br>- основные методы организационного обеспечения информационной безопасности специальных АИС | 04, Построение системы ИБ; 05, Информационные системы (ИС) и обеспечение их безопасности; 06, Создание архитектуры информационно-аналитических систем (ИАС) | Устный опрос |
| | уметь:<br>- применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем | 04, Построение системы ИБ; 05, Информационные системы (ИС) и обеспечение их безопасности; 06, Создание архитектуры информационно-аналитических систем (ИАС) | Устный опрос |
| | владеть:<br>- навыками анализа и синтеза структурных и функциональных схем технологических процессов обработки | 04, Построение системы ИБ; 05, Информационные системы (ИС) и обеспечение их безопасности; 06, | Практическое задание |

| | | | |
|---|---|---|---|
| | информации в специальных АИС;<br>- навыками выбора и обоснования критериев эффективности функционирования специальных АИС | Создание архитектуры информационно-аналитических систем (ИАС) | |
| ПК-13: способность оценивать эффективность специальных ИАС, в том числе средств обеспечения их информационной безопасности | знать:<br>- методологические основы, методы и средства моделирования специальных АИС;<br>- методы построения и исследования математических моделей специальных АИС;<br>- методы планирования и оптимизации компьютерных экспериментов с моделями специальных АИС;<br>- методологические основы, методы и средства построения распределенных специальных АИС; системы распределенной обработки данных, используемые в специальных АИС;<br>- нормативную базу, регламентирующую создание и эксплуатацию специальных АИС | 04, Построение системы ИБ; 06, Создание архитектуры информационно-аналитических систем (ИАС) | Устный опрос |
| | уметь:<br>- осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты;<br>- пользоваться средствами защиты, предоставляемыми системами управления базами данных | 06, Создание архитектуры информационно-аналитических систем (ИАС) | Устный опрос |
| | владеть:<br>- навыками анализа программных | 06, Создание архитектуры информационно- | Практическое задание |

| | | | |
|---|---|---|---|
| | реализаций;<br>- методами моделирования безопасности компьютерных систем, в том числе, моделирования управления доступом и информационными потоками в компьютерных системах | аналитических систем (ИАС) | |

**19.2. Описание критериев и шкалы оценивания компетенций (результатов обучения) при промежуточной аттестации)**

Для оценивания результатов обучения на зачёте (с оценкой) используются следующие показатели:

- Знание сущности и понятие информации, информационной безопасности и характеристику ее составляющих; основных средств и способов обеспечения информационной безопасности, принципов построения систем защиты информации; принципов построения и основные виды симметричных и асимметричных криптографических алгоритмов; основных методов организационного обеспечения информационной безопасности специальных АИС; структуры функциональной и обеспечивающих частей специальных АИС; методов проектирования АИС.

- Умение применять осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты; пользоваться средствами защиты, предоставляемыми системами управления базами данных.

- Владение навыками исследования математических моделей технологических процессов обработки информации в специальных АИС с целью оценки качества и оптимизации характеристик специальных АИС; навыками выбора и обоснования критериев эффективности функционирования специальных АИС; методами и средствами выявления угроз безопасности компьютерным системам; методами моделирования безопасности компьютерных систем, в том числе, моделирования управления доступом и информационными потоками в компьютерных системах.

| Критерии оценивания компетенций | Уровень сформированности компетенций | Шкала оценок |
|---|---|---|
| Глубокие исчерпывающие знания всего программного материала, понимание сущности и взаимосвязи рассматриваемых процессов и явлений. Логически последовательные, полные, правильные и конкретные ответы на | Пороговый уровень и выше порогового | Отлично |

| | | |
|---|---|---|
| все основные вопросы. Правильные и конкретные ответы дополнительные вопросы. | | |
| Твердые и достаточно полные знания программного материала, понимание сущности рассматриваемых процессов и явлений. Последовательные и правильные, но недостаточно развернутые ответы на основные вопросы. Правильные ответы на дополнительные вопросы. | Пороговый уровень и выше порогового | Хорошо |
| Правильные и конкретные, без грубых ошибок ответы на основные вопросы. Наличие отдельных неточностей в ответах. В целом правильные ответы с небольшими неточностями на дополнительные вопросы. | Пороговый уровень | Удовлетворительно |
| Плохое владение материалом: ответ неверен, отсутствие ориентации в предмете, когда количество неправильных ответов превышает количество допустимых для положительной оценки. | Ниже порогового уровня | Неудовлетворительно |

**19.3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций в процессе освоения образовательной программы**

*Примерный перечень заданий проверки практических навыков*

1. Привести пример действия атакующего и способ защиты от атаки «man-in-the-middle».
2. Привести пример структуры и функциональности стека протоколов TCP/IP.
3. Применить алгоритм кластеризации по заданной модели.
4. Подсчитать метрику релевантности информационного сообщения по данным профиля и микроблога конкретного пользователя сети.
5. Определить скорость распространения информации по имитационной модели распространения информации в социальной сети на выбор (SIS. SIR, SIDR).
6. Рассчитать среднее значение кластерного коэффициента для большого графа программным методом.
7. Создать класс-обёртку для вызова API функций социальных сетей.
8. Провести ROC-анализ на заданной регрессионной модели.
9. Описать методы функции Data Mining.

*Примерный перечень вопросов к зачёту*

1. Основные понятия защиты информации и информационной безопасности.

2. Анализ угроз информационной безопасности.
3. Модель ISO/OSI и стек протоколов TCP/IP.
4. Проблемы безопасности IP-сетей.
5. Угрозы и уязвимости проводных корпоративных сетей.
6. Угрозы и уязвимости проводных беспроводных сетей.
7. Способы обеспечения информационной безопасности.
8. Пути решения проблем защиты в информационных сетях.
9. Структура политики безопасности.
10. Базовая политика безопасности.
11. Специализированные политики безопасности.
12. Процедуры безопасности.
13. Стандарты информационной безопасности и их роль.
14. Стандарты ISO/IEC 17799:2002.
15. Стандарт BS1 (Германия).
16. Международный стандарт ISO 15408.
17. Стандарты безопасности беспроводных сетей.
18. Стандарты информационной безопасности в Интернете.
19. Стандарты безопасности информационных технологий РФ.
20. Основные понятия криптографии.
21. Симметричные криптосистемы шифрования.
22. Асимметричные криптосистемы шифрования.
23. Комбинированная криптосистема шифрования.
24. Основные процедуры цифровой подписи.
25. Управление криптоключами.
26. Классификация криптографических алгоритмов.
27. Основные методы аутентификации.
28. Межсетевой экран. Фильтрация трафика. Прикладной шлюз.
29. Виртуальная сеть VPN. Средства обеспечения безопасности.
30. Анализ защищённости и обнаружение атак. Концепция адаптивного управления.
31. Средства анализа защищённости ОС.
32. Классификация систем обнаружения атак IDS.
33. Классификация компьютерных вирусов.

**19.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций**

Оценка знаний, умений и навыков, характеризующая этапы формирования компетенций в рамках изучения дисциплины осуществляется в ходе текущей и промежуточной аттестаций.

Текущая аттестация проводится в форме письменно-устного опроса (индивидуального).

Промежуточная аттестация включает в себя теоретические вопросы, позволяющие оценить уровень полученных знаний и защиту контрольной работы, позволяющую оценить степень сформированности умений и навыков.

При оценивании используются качественные шкалы оценок. Критерии оценивания приведены выше.