

Документ подписан простой электронной подписью
Информация о владельце:

ФИО: Иванов Е.А.

Должность: Ректор

Дата подписания: 24.04.2023 09:39:14

Уникальный программный ключ:

c098bc0c1041cb2a4cf926cf171d6715d99a6ae00adc8e27b55cbe1e2dbd7c78

Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования «Ростовский государственный экономический университет (РИНХ)»

УТВЕРЖДАЮ

Директор Института магистратуры

 Иванова Е.А.

« 29 » 08 2022 г.

**Рабочая программа дисциплины
Экспертиза вычислительной техники и компьютерных носителей информации**

Направление 10.04.01 Информационная безопасность
магистерская программа 10.04.01.02 "Программно-аппаратные методы расследования
компьютерных преступлений"

Для набора 2022 года

Квалификация
магистр


КАФЕДРА **Информационные технологии и защита информации**

Распределение часов дисциплины по семестрам


| Семестр (<Курс>.<Семестр на курсе>) | 3 (2.1) | | Итого | |
|---|---------|-----|-------|-----|
| | 15 2/6 | | | |
| Неделя | уп | рп | уп | рп |
| Лекции | 16 | 16 | 16 | 16 |
| Лабораторные | 32 | 32 | 32 | 32 |
| Практические | 32 | 32 | 32 | 32 |
| Итого ауд. | 80 | 80 | 80 | 80 |
| Контактная работа | 80 | 80 | 80 | 80 |
| Сам. работа | 28 | 28 | 28 | 28 |
| Итого | 108 | 108 | 108 | 108 |

ОСНОВАНИЕ

Учебный план утвержден учёным советом вуза от 22.02.2022 протокол № 7.

Программу составил(и): д.э.н., проф., Тищенко Е.Н. 

Зав. кафедрой: к.э.н., доцент Ефимова Е.В. 

Методическим советом направления: д.э.н., профессор, Тищенко Е.Н. 

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

| | |
|-----|--|
| 1.1 | Освоение дисциплинарных компетенций, связанных проведением экспертизы вычислительной техники и компьютерных носителей информации |
|-----|--|

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

ПК-4:Способен осуществлять анализ результатов экспериментальных исследований с применением математических и физических методов, выбор технических средств инструментального мониторинга защищенности объектов информатизации

В результате освоения дисциплины обучающийся должен:

Знать:

нормативно-правовые акты, методические документы, стандарты в области обеспечения информационной безопасности и аттестации объектов информатизации(соотнесено с индикатором ПК-4.1.)

Уметь:

разрабатывать программы и методики, проводить аудирование и аттестационные испытания объектов информатизации на соответствие требованиям обеспечения информационной безопасности;
оформлять материалы аудита и аттестационных испытаний (соотнесено с индикатором ПК-4.2.)

Владеть:

навыками разработки программ и методик проведения аудирования и аттестационных испытаний объектов информатизации;навыками подготовки заключения по результатам аудита и аттестации объектов информатизации (соотнесено с индикатором ПК-4.3.)

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

| Код занятия | Наименование разделов и тем /вид занятия/ | Семестр / Курс | Часов | Компетенции | Литература |
|-------------|--|----------------|-------|-------------|------------------------------|
| | Раздел 1. Этапы проведения экспертизы | | | | |
| 1.1 | Понятие и структура автоматизированной экспертной системы. Принципы оценки информационной безопасности автоматизированных информационных и телекоммуникационных систем. Структура и функции экспертной системы комплексной оценки информационной безопасности. Классификация экспертных систем оценки информационной безопасности. /Лек/ | 3 | 2 | ПК-4 | Л1.1 Л1.2Л2.1 Л2.2 Л2.3 |
| 1.2 | "Общая теория экспертных систем комплексной оценки информационной безопасности". Создание классификации существующих экспертных систем на основе анализа результатов поиска в сети Интернет. /Лаб/ | 3 | 14 | ПК-4 | Л1.1 Л1.2Л2.1 Л2.2 Л2.3 |
| 1.3 | "Общая теория экспертных систем комплексной оценки информационной безопасности". Создание классификации существующих экспертных систем на основе анализа результатов поиска в сети Интернет. /Пр/ | 3 | 4 | ПК-4 | Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 |
| 1.4 | "Общая теория экспертных систем комплексной оценки информационной безопасности". ПрЦели, задачи и функции экспертных систем оценки ИБ. Типы экспертных систем оценки ИБ. Классификация. Отличительные признаки информации, применимой для анализа в экспертных системах оценки ИБ. /Ср/ | 3 | 4 | ПК-4 | Л1.1 Л1.2Л2.1 Л2.2 Л2.3 |

| | | | | | |
|-----|--|---|----|------|---------------------------------|
| 1.5 | Тема 2. "Данные для анализа в экспертных системах". Типы, классификация, сбор и подготовка данных. Особенности и основные отличительные признаки необходимых данных об исследуемой автоматизированной системе. Типы данных, их представление в разных подсистемах экспертной системы. Классы данных. Методы сбора и подготовки данных для обработки в экспертной системе. Методы анализа данных. /Лек/ | 3 | 2 | ПК-4 | Л1.1 Л1.2Л2.1 Л2.2 Л2.3 |
| 1.6 | Тема 2. "Данные для анализа в экспертных системах". Процедуры и программы сбора данных о подсистеме защиты информации автоматизированной системы. Основные требования. Функции-обработчики данных в экспертной системе оценки ИБ. Математический аппарат, применяемый в обработчиках. /Пр/ | 3 | 6 | ПК-4 | Л1.1 Л1.2Л2.1 Л2.2 Л2.3 |
| | Раздел 2. Экспертные информационные системы в комплексном анализе информационной безопасности автоматизированных систем | | | | |
| 2.1 | "Программные и аппаратные средства экспертных систем комплексной оценки информационной безопасности". Программные средства экспертных систем: процедуры и программы сбора данных о подсистеме защиты информации автоматизированной системы, функции-обработчики данных, базы данных, элементы искусственного интеллекта для анализа полученных данных и синтеза решений. Аппаратные средства экспертных систем: средства сбора информации, средства обработки информации. /Лек/ | 3 | 4 | ПК-4 | Л1.1 Л1.2Л2.1 Л2.2 Л2.3 |
| 2.2 | "Программные и аппаратные средства экспертных систем комплексной оценки информационной безопасности". Системы показателей защищенности (эффективности). Метод оценки эффективности на основе структурных вопросников. Метод групповых экспертных оценок. /Лаб/ | 3 | 4 | ПК-4 | Л1.1 Л1.2Л2.1 Л2.2 Л2.3 |
| 2.3 | "Программные и аппаратные средства экспертных систем комплексной оценки информационной безопасности". Системы показателей защищенности (эффективности). Метод оценки эффективности на основе структурных вопросников. Метод групповых экспертных оценок. /Пр/ | 3 | 6 | ПК-4 | Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 |
| 2.4 | "Программные и аппаратные средства экспертных систем комплексной оценки информационной безопасности". Блоки принятия решений. Элементы искусственного интеллекта для анализа полученных данных и синтеза решений. Подходы к комплексной оценке ИБ автоматизированной системы. Различия для информационных и телекоммуникационных систем. Российские и международные стандарты, применяемые для оценки ИБ автоматизированной системы. Этапы проектирования экспертных систем оценки ИБ. Жизненный цикл экспертных систем. Принципы тестирования автоматизированных систем при помощи экспертных систем оценки ИБ. /Ср/ | 3 | 12 | ПК-4 | Л1.1 Л1.2Л2.1 Л2.2 Л2.3 |
| 2.5 | "Методы проектирования экспертных систем комплексной оценки ИБ". Основные подсистемы экспертной системы комплексной оценки ИБ. Подходы к проектированию экспертных систем. Особенности проектирования систем комплексной оценки ИБ. Общая методика проектирования экспертных систем оценки ИБ. Особенности тестирования автоматизированных систем при помощи экспертных систем оценки ИБ, достоверность оценки ИБ. /Лек/ | 3 | 4 | ПК-4 | Л1.1 Л1.2Л2.1 Л2.2 Л2.3 |

| | | | | | |
|------|---|---|----|------|---------------------------------|
| 2.6 | "Методы проектирования экспертных систем комплексной оценки ИБ". Обработки экспертных оценок безопасности информации в информационных и телекоммуникационных системах различными методами. Сравнительная оценка методов. /Лаб/ | 3 | 6 | ПК-4 | Л1.1 Л1.2Л2.1 Л2.2 Л2.3 |
| 2.7 | Системы контроля инцидентов ИБ как вариант экспертных систем оценки безопасности. Развитие экспертных систем оценки ИБ автоматизированных информационных и телекоммуникационных систем. /Пр/ | 3 | 6 | ПК-4 | Л1.1 Л1.2Л2.1 Л2.2 Л2.3 |
| 2.8 | Тема 5. "Современные экспертные системы комплексной оценки ИБ". Системы комплексного аудита информационной безопасности автоматизированных систем. Сканеры информационной безопасности. Экспертные системы оценки информационной безопасности автоматизированных систем на основе искусственного интеллекта. /Лек/ | 3 | 4 | ПК-4 | Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 |
| 2.9 | "Современные экспертные системы комплексной оценки ИБ". Выработка рекомендаций по совершенствованию информационной безопасности на основе экспертных оценок. Работа в LibreProject. /Лаб/ | 3 | 4 | ПК-4 | Л1.1 Л1.2Л2.1 Л2.2 Л2.3 |
| 2.10 | Стандарты проведения. Экспертные системы оценки ИБ как средства проведения аудита. Сканеры безопасности как пример экспертных систем оценки ИБ. Общая характеристика. Типы и принципы работы сканеров ИБ. /Пр/ | 3 | 4 | ПК-4 | Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 |
| 2.11 | "Современные экспертные системы комплексной оценки ИБ". Аудит ИБ. Классификация. Стандарты проведения. Экспертные системы оценки ИБ как средства проведения аудита. Сканеры безопасности как пример экспертных систем оценки ИБ. Общая характеристика. Типы и принципы работы сканеров ИБ. Проведение оценки ИБ системы на примере одного из существующих сканеров. Особенности аудита операционных систем и программного обеспечения. Отчет по проведенному аудиту. Правила и особенности. Автоматизация составления отчетов экспертных систем оценки ИБ. /Ср/ | 3 | 12 | ПК-4 | Л1.1 Л1.2Л2.1 Л2.2 Л2.3 |
| 2.12 | Проведение оценки ИБ системы на примере одного из существующих сканеров. Особенности аудита операционных систем и программного обеспечения. Отчет по проведенному аудиту. Правила и особенности. Автоматизация составления отчетов экспертных систем оценки ИБ. /Лаб/ | 3 | 4 | ПК-4 | Л1.1 Л1.2Л2.2 Л2.3 Л2.4 |
| 2.13 | Проведение оценки ИБ системы на примере одного из существующих сканеров. Особенности аудита операционных систем и программного обеспечения. Отчет по проведенному аудиту. Правила и особенности. Автоматизация составления отчетов экспертных систем оценки ИБ. /Пр/ | 3 | 6 | ПК-4 | Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 |
| 2.14 | /Зачёт/ | 3 | 0 | ПК-4 | Л1.1 Л1.2Л2.1 Л2.2 Л2.3 |

4. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Структура и содержание фонда оценочных средств для проведения текущей и промежуточной аттестации представлены в Приложении 1 к рабочей программе дисциплины.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Основная литература

| Авторы, составители | Заглавие | Издательство, год | Колич-во |
|---------------------|----------|-------------------|----------|
|---------------------|----------|-------------------|----------|

| | Авторы, составители | Заглавие | Издательство, год | Колич-во |
|------|---|---|--|---|
| Л1.1 | Заляжных, В. А., Гирик, А. В. | Экспертные системы комплексной оценки безопасности автоматизированных информационных и коммуникационных систем | Санкт-Петербург: Университет ИТМО, 2014 | http://www.iprbookshop.ru/65733.html неограниченный доступ для зарегистрированных пользователей |
| Л1.2 | Кубашева Е. С., Малашкевич И. А., Чекулаева Е. Н. | Информатика и вычислительная техника. Информационная безопасность автоматизированных систем: учебно-методическое пособие к прохождению производственной практики: учебно-методическое пособие | Йошкар-Ола: Поволжский государственный технологический университет, 2019 | https://biblioclub.ru/index.php?page=book&id=562246 неограниченный доступ для зарегистрированных пользователей |

5.2. Дополнительная литература

| | Авторы, составители | Заглавие | Издательство, год | Колич-во |
|------|--|---|---|---|
| Л2.1 | Мельников В. П., Клейменов С. А., Петраков А. М., Клейменов С. А. | Информационная безопасность и защита информации: учеб. пособие для студентов вузов, обучающихся по спец. "Информ. системы и технологии" | М.: Академия, 2012 | 20 |
| Л2.2 | Баранова Е. К., Бабаш А. В. | Информационная безопасность и защита информации: учеб. пособие | М.: РИО♦, 2014 | 11 |
| Л2.3 | | Информационная безопасность: журнал | Москва: Гротек, 2014 | https://biblioclub.ru/index.php?page=book&id=364894 неограниченный доступ для зарегистрированных пользователей |
| Л2.4 | Богомолова, М. А. | Экспертные системы (техника и технология проектирования): методические указания к лабораторным работам | Самара: Поволжский государственный университет телекоммуникаций и информатики, 2015 | http://www.iprbookshop.ru/71908.html неограниченный доступ для зарегистрированных пользователей |

5.3 Профессиональные базы данных и информационные справочные системы

| |
|---|
| СПС КонсультантПлюс |
| СПС Гарант |
| ЭБС «IPR Books» http://www.iprbookshop.ru/ |
| Библиоклуб.ру http://biblioclub.ru/ |

5.4. Перечень программного обеспечения

| |
|--------------|
| LibreProject |
|--------------|

5.5. Учебно-методические материалы для студентов с ограниченными возможностями здоровья

При необходимости по заявлению обучающегося с ограниченными возможностями здоровья учебно-методические материалы предоставляются в формах, адаптированных к ограничениям здоровья и восприятия информации. Для лиц с нарушениями зрения: в форме аудиофайла; в печатной форме увеличенным шрифтом. Для лиц с нарушениями слуха: в форме электронного документа; в печатной форме. Для лиц с нарушениями опорно-двигательного аппарата: в форме электронного документа; в печатной форме.

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

| |
|---|
| Помещения для всех видов работ, предусмотренных учебным планом, укомплектованы необходимой специализированной учебной мебелью и техническими средствами обучения: |
| - столы, стулья; |
| - персональный компьютер / ноутбук (переносной); |
| - проектор, экран / интерактивная доска. |
| Лабораторные занятия проводятся в компьютерных классах, рабочие места в которых оборудованы необходимыми лицензионными и/или свободно распространяемыми программными средствами и выходом в Интернет. |

7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

| |
|--|
| Методические указания по освоению дисциплины представлены в Приложении 2 к рабочей программе дисциплины. |
|--|

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

1 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

1.1 Показатели и критерии оценивания компетенций:

| ЗУН, составляющие компетенцию | Показатели оценивания | Критерии оценивания | Средства оценивания |
|---|--|--|------------------------------------|
| ПК-4: способен осуществлять анализ результатов экспериментальных исследований с применением математических и физических методов, выбор технических средств инструментального мониторинга защищенности объекта информатизации | | | |
| З. нормативно-правовые акты, методические документы, стандарты в области обеспечения информационной безопасности и аттестации объектов информатизации(соотнесено с индикатором ПК-4.1.) | поиск и сбор необходимой литературы, использование различных баз данных | полнота и содержательность ответа умение приводить примеры | Т (1-14) З (1-30) |
| У. разрабатывать программы и методики, проводить аудирование и аттестационные испытания объектов информатизации на соответствие требованиям обеспечения информационной безопасности; оформлять материалы аудита и аттестационных испытаний (соотнесено с индикатором ПК-4.2.) | использование информационных технологий в практической деятельности для приобретения новых знаний и умений | полнота и содержательность ответа умение приводить примеры умение самостоятельно находить решение поставленных задач | ЛЗ (1-5) ПЗ (1-4) ПОЗЗ (1-5) |
| В. навыками разработки программ и методик проведения аудирования и аттестационных испытаний объектов информатизации;навыками подготовки заключения по результатам аудита и аттестации объектов информатизации (соотнесено с индикатором ПК-4.3.) | использование современных информационно-коммуникационных технологий и различных информационных ресурсов | полнота и содержательность ответа умение приводить примеры | ЛЗ (1-5) ПОЗЗ (1-5) ПЗ (1-4) |

*ЛЗ – лабораторное задания, Т – тест, З – вопросы к зачету, ПОЗЗ – практико-ориентированные задания к зачету
ПЗ –практические задания*

1.2 Шкалы оценивания:

Текущий контроль успеваемости и промежуточная аттестация осуществляется в рамках накопительной балльно-рейтинговой системы в 100-балльной шкале.

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

Вопросы к зачету

1. Понятие экспертной системы. Особенности экспертных систем оценки информационной безопасности.
2. Принципы и подходы к комплексной оценке информационной безопасности в экспертных системах.
3. Общая структура экспертных систем оценки ИБ.
4. Классификация экспертных систем оценки информационной безопасности.
5. Цели, задачи и функции экспертных систем оценки ИБ.
6. Типы экспертных систем оценки ИБ. Классификация.
7. Отличительные признаки информации, применимой для анализа в экспертных системах оценки ИБ.
8. Классификация и типы используемых данных. Порядок работы с данными в экспертной системе ИБ.
9. Аппаратное обеспечение экспертной системы оценки ИБ. Основные требования. Стандарты.
10. Аппаратные средства сбора и обработки данных в экспертных системах оценки ИБ. Примеры.
11. Программное обеспечение экспертной системы оценки ИБ. Классификация. Стандарты.
12. Процедуры и программы сбора данных о подсистеме защиты информации автоматизированной системы. Основные требования.
13. Функции-обработчики данных в экспертной системе оценки ИБ. Математический аппарат, применяемый в обработчиках.
14. Базы данных для экспертных систем оценки ИБ. Особенности взаимодействия интерфейсов экспертной системы с базами данных.
15. Блоки принятия решений. Элементы искусственного интеллекта для анализа полученных данных и синтеза решений.
16. Подходы к комплексной оценке ИБ автоматизированной системы. Различия для информационных и телекоммуникационных систем.
17. Российские и международные стандарты, применяемые для оценки ИБ автоматизированной системы.
18. Этапы проектирования экспертных систем оценки ИБ. Жизненный цикл экспертных систем.
19. Принципы тестирования автоматизированных систем при помощи экспертных систем оценки ИБ.
20. Оценка достоверности полученных результатов. Математические методы оценки достоверности результатов работы экспертных систем оценки ИБ.
21. Аудит ИБ. Классификация. Стандарты проведения.
22. Экспертные системы оценки ИБ как средства проведения аудита.
23. Сканеры безопасности как пример экспертных систем оценки ИБ. Общая характеристика.
24. Типы и принципы работы сканеров ИБ. Проведение оценки ИБ системы на примере одного из существующих сканеров.
25. Особенности аудита операционных систем и программного обеспечения.
26. Отчет по проведенному аудиту. Правила и особенности.
27. Автоматизация составления отчетов экспертных систем оценки ИБ. 28. Экспертные системы оценки ИБ на предприятии. Особенности эксплуатации.
29. Системы контроля инцидентов ИБ как вариант экспертных систем оценки безопасности.
30. Развитие экспертных систем оценки ИБ автоматизированных информационных и телекоммуникационных систем.

Практико-ориентированные задания к зачету

1. Установить угрозы, атаки и риски сетевой безопасности.
2. Установить антивирусное программное обеспечение.
3. Установить Linux-подобную операционную систему.
4. Настроить впервые установленную Linux-подобную операционную систему.
5. Установить шифровальную систему.

Ключ для контроля правильности выполнения практических заданий к экзамену

Установить угрозы, атаки и риски сетевой безопасности:

Установить шифровальную систему.



Шкалы оценивания:

Тесты

1. Как называлась первая экспертная система?
 - a) MACSYMA
 - b) EMYCIN
 - c) PROSPECTOR
 - d) нет правильного ответа
2. Какую задачу решала экспертная система PROSPECTOR?
 - a) определение наиболее вероятной структуры химического соединения
 - b) поиск месторождений на основе геологических анализов
 - c) диагностика глазных заболеваний
 - d) распознавание слитной человеческой речи
 - e) нет правильного ответа
3. Какая экспертная система разрабатывается 1-1,5 года?
 - a) исследовательский образец
 - b) демонстрационная
 - c) коммерческая
 - d) нет правильного ответа
4. Какая экспертная система имеет базу знаний размером от 1000 до 10000 структурированных правил?
 - a) простая
 - b) средняя
 - c) сложная
5. Какие подсистемы являются для экспертной системы обязательными?
 - a) база знаний
 - b) интерфейс системы с внешним миром
 - c) алгоритмические методы решений
 - d) интерфейс когнитолога
 - e) контекст предметной области
6. Характерной особенностью экспертной системы является наличие базы
 - a) да
 - b) нет
7. Для решения каких задач предназначены статические оболочки экспертных систем?
 - a) для управления и диагностики в режиме реального времени
 - b) для решения статических задач
 - c) для решения задач анализа и синтеза с разделением времени
 - d) для разработки динамических систем
 - e) нет правильного ответа
8. Гибридная экспертная система подразумевает:
 - a) использование нескольких средств разработки
 - b) использование различных подходов к программированию
 - c) использование нескольких методов представления знаний
 - d) нет правильного ответа
9. Кто создает базу знаний экспертной системы?

- a) программист
- b) пользователь
- c) когнитолог
- d) эксперт

10. Увеличение объема базы знаний может быть причиной перепроектирования ЭС

- a) да
- b) нет

11. Целостность и наглядность описания предметной области сохраняется в семантических сетях с увеличением размеров и усложнением связей

- a) да
- b) нет

12. Экспертные системы применимы для решения задач планирования

- a) да
- b) нет

13. Компьютеры в виде систем искусственного интеллекта рожают социальный интеллект как единую целенаправленную творческую систему

- a) да
- b) нет

14. Задачи аппаратного моделирования деятельности человека могут относиться к задачам искусственного интеллекта

- a) да
- b) нет

Тестовое задание выполняется на отдельном листе. Лист подписывается ФИО, номер группы, номер зачетной книжки, указывается вариант тестового задания. Ниже обучающийся указывает цифрой номер вопроса и рядом ставит номер правильного, на его взгляд, варианта ответа. Тестовое задание содержит 10 вопросов с вариантами ответов. Если обучающийся до сдачи преподавателю тестового задания и листа с ответами, считает, что не правильно ответил на тот или иной вопрос теста, то зачеркивает предыдущий вариант ответа и рядом указывает новый. За ошибку это не считается. Время прохождения тестирования 20 минут. После окончания выполнения тестового задания обучающийся сдает преподавателю вариант тестового задания и лист с ответами.

Критерии оценки:

- 1-10 баллов выставляется обучаемому. За один правильный ответ обучаемый получает 1 балл.

Лабораторные задания

Лабораторное задание 1. Создание классификации существующих экспертных систем на основе анализа результатов поиска в сети Интернет.

Лабораторное задание 2. Сравнительный анализ подходов оценки эффективности систем защиты информации.

Классификационная структура методов и моделей оценки эффективности комплексной системы защиты информации.

Работа в ProjectExpert 7.

Лабораторное задание 3. Системы показателей защищенности (эффективности). Метод оценки эффективности на основе структурных вопросников. Метод групповых экспертных оценок. Системы показателей защищенности (эффективности).

Метод оценки эффективности на основе структурных вопросников. Метод групповых экспертных оценок.

Лабораторное задание 4. Обработки экспертных оценок безопасности информации в информационных и телекоммуникационных системах различными методами. Сравнительная оценка методов.

Лабораторное задание 5. Выработка рекомендаций по совершенствованию информационной безопасности на основе экспертных оценок.

Критерии оценки:

(для каждого задания):

10 б. – задание выполнено верно;

9-8 б. – при выполнении задания были допущены неточности, не влияющие на результат;

7-5 б. – при выполнении задания были допущены ошибки;

4-1 б. – при выполнении задания были допущены существенные ошибки

0 б. – задание не выполнено.

Практические задания

1. "Программные и аппаратные средства экспертных систем комплексной оценки информационной безопасности". Системы показателей защищенности (эффективности). Метод оценки эффективности на основе структурных вопросников. Метод групповых экспертных оценок.
2. Системы контроля инцидентов ИБ как вариант экспертных систем оценки безопасности. Развитие экспертных систем оценки ИБ автоматизированных информационных и телекоммуникационных систем.
3. Стандарты проведения. Экспертные системы оценки ИБ как средства проведения аудита. Сканеры безопасности как пример экспертных систем оценки ИБ. Общая характеристика. Типы и принципы работы сканеров ИБ.
4. Проведение оценки ИБ системы на примере одного из существующих сканеров. Особенности аудита операционных систем и программного обеспечения. Отчет по проведенному аудиту. Правила и особенности. Автоматизация составления отчетов экспертных систем оценки ИБ.

Критерии оценки:

(для каждого задания):

10 б. – задание выполнено верно;

9-8 б. – при выполнении задания были допущены неточности, не влияющие на результат;

7-5 б. – при выполнении задания были допущены ошибки;

4-1 б. – при выполнении задания были допущены существенные ошибки

0 б. – задание не выполнено.

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

Процедуры оценивания включают в себя текущий контроль и промежуточную аттестацию.

Текущий контроль успеваемости проводится с использованием оценочных средств, представленных в п. 2 данного приложения. Результаты текущего контроля доводятся до сведения студентов до промежуточной аттестации.

Зачет проводится по расписанию промежуточной аттестации.

Количество вопросов в задании – 3. Объявление результатов производится в день зачета. Результаты аттестации заносятся в зачетную ведомость и зачетную книжку студента. Студенты, не прошедшие промежуточную аттестацию по графику, должны ликвидировать задолженность в установленном порядке.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Учебным планом предусмотрены следующие виды занятий:

- лекции;
- лабораторные занятия
- практические занятия.

В ходе лекционных занятий рассматриваются вопросы, связанные с проведением экспертизы вычислительной техники, даются рекомендации для самостоятельной работы и подготовке к практическим и лабораторным занятиям.

В ходе практических и лабораторных занятий углубляются и закрепляются знания студентов по ряду рассмотренных на лекциях вопросов, развиваются навыки комплексной оценки безопасности автоматизированных информационных и телекоммуникационных систем.

При подготовке к лабораторным и практическим занятиям каждый студент должен:

- изучить рекомендованную учебную литературу;
- изучить конспекты лекций;
- подготовить ответы на все вопросы по изучаемой теме;
- письменно решить домашнее задание, рекомендованные преподавателем при изучении каждой темы.

В процессе подготовки к лабораторным и практическим занятиям студенты могут воспользоваться консультациями преподавателя.

Вопросы, не рассмотренные на лекциях и лабораторных занятиях, должны быть изучены студентами в ходе самостоятельной работы. Контроль самостоятельной работы студентов над учебной программой курса осуществляется в ходе занятий посредством тестирования. В ходе самостоятельной работы каждый студент обязан прочитать основную и по возможности дополнительную литературу по изучаемой теме, дополнить конспекты лекций недостающим материалом, выписками из рекомендованных первоисточников. Выделить непонятные термины, найти их значение в энциклопедических словарях.

Для подготовки к занятиям, текущему контролю и промежуточной аттестации студенты могут воспользоваться электронно-библиотечными системами. Также обучающиеся могут взять на дом необходимую литературу на абонементе университетской библиотеки или воспользоваться читальными залами.