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.
«01» июня 2023г.

Рабочая программа дисциплины
Управление информационной безопасностью

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

Для набора 2023 года

Квалификация
магистр

КАФЕДРА **Информационная безопасность**

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**1 (1.1)**		Итого	
Недель	15 2/6			
Вид занятий	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
Часы на контроль	36	36	36	36
Итого	144	144	144	144

ОСНОВАНИЕ

Учебный план утвержден учёным советом вуза от 28.03.2023 протокол № 9.

Программу составил(и): к.т.н., доцент, Лапсарь А.П.

Зав. кафедрой: к.э.н., Радченко Ю.В.

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

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1	получение обучаемыми теоретических знаний по организации управления информационной безопасностью на объектах информатизации и в организациях, использующих в своей деятельности информационные системы; изучение и последующее освоение современных технологий защиты информации ограниченного доступа на объектах; оптимизация организационных и технических мероприятий по обеспечению информационной безопасности организации

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

УК-3:Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели

ОПК-3:Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности;

В результате освоения дисциплины обучающийся должен:

Знать:

методики формирования команд;методы эффективного руководства коллективами.(соотнесено с индикатором УК-3.1.)
основы отечественных и зарубежных стандартов в области сертификации и аттестации объектов информатизации, в области управления информационной безопасностью с целью разработки проектов организационно-распорядительных документов (соотнесено с индикатором ОПК-3.1.)

Уметь:

разрабатывать командную стратегию; организовывать работу коллективов; управлять коллективом;разрабатывать мероприятия по личностному, образовательному и профессиональному росту(соотнесено с индикатором УК-3.2.)
разрабатывать технические задания на создание подсистем обеспечения информационной безопасности.(соотнесено с индикатором ОПК-3.2.)

Владеть:

методами организации и управления коллективом, планированием его действий.(соотнесено с индикатором УК-3.3.)
навыками разработки политик безопасности различных уровней.(соотнесено с индикатором ОПК-3.3.)

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Раздел 1. Системы управления информационной безопасности

№	Наименование темы / Вид занятия	Семестр	Часов	Компетенции	Литература
1.1	Тема 1 "Основные положения теории информационной безопасности». Исследование архитектуры построения систем управления информационной безопасностью. Оформление при помощи LibreOffice / Лаб /	1	4	ОПК-3,УК- 3	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
1.2	Тема 1 "Основные положения теории информационной безопасности». Исследование архитектуры построения систем управления информационной безопасностью. / Лек /	1	4	ОПК-3,УК- 3	Л1.1, Л1.2, Л1.3, Л2.3, Л2.5
1.3	Тема 1 "Основные положения теории информационной безопасности». Управление информационной безопасностью объекта информатизации. / Пр /	1	6	ОПК-3,УК- 3	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.4, Л2.5
1.4	Тема 1 "Основные положения теории информационной безопасности». Информационная безопасность: основные определения. Понятие конфиденциальности, целостности, доступности информации. Формальные модели управления доступом: модель Харрисона-Руззо-Ульмана, модель Белла Ла-Падулы. Формальные модели целостности: модель Кларка-Вилсона, модель Биба. Совместное использование моделей безопасности. Ролевое управление доступом. / Ср /	1	10	ОПК-3,УК- 3	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
1.5	«Угрозы информационной безопасности. Теоретические основы построения систем защиты от угроз». Исследование свойств локальной политики безопасности. / Лек /	1	4	ОПК-3,УК- 3	Л1.2, Л1.3, Л2.3, Л2.5
1.6	Тема 2 «Угрозы информационной безопасности. Теоретические основы построения систем защиты от угроз». Исследование свойств локальной политики безопасности. Оформление при помощи MS Office / Лаб /	1	4	ОПК-3,УК- 3	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5

1.7	Тема 2 «Угрозы информационной безопасности. Теоретические основы построения систем защиты от угроз». Управление средствами защиты информации на объекте. / Пр /	1	6	ОПК-3,УК- 3	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.4, Л2.5
1.8	Тема 2 «Угрозы информационной безопасности. Теоретические основы построения систем защиты от угроз». Классификация угроз информационной безопасности. Построение систем защиты от угроз нарушения конфиденциальности информации: модель системы защиты, организационное обеспечение ИБ, идентификация и аутентификация, разграничение доступа, криптографические методы, контроль внешнего периметра, протоколирование, аудит. Построение систем защиты от угроз нарушения целостности информации: модель обеспечения целостности, криптографические методы. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем. / Ср /	1	4	ОПК-3,УК- 3	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5

Раздел 2. Методы и технологии информационной безопасности

№	Наименование темы / Вид занятия	Семестр	Часов	Компетенции	Литература
2.1	"Информационное противоборство, методы и средства его ведения. Методы и средства обеспечения информационной безопасности объектов информационной сферы». Исследование функционирования систем управления информационной безопасностью на объекте защиты. / Лек /	1	4	ОПК-3,УК- 3	Л1.1, Л1.2, Л1.3, Л2.3, Л2.5
2.2	Тема 1 "Информационное противоборство, методы и средства его ведения. Методы и средства обеспечения информационной безопасности объектов информационной сферы». Исследование функционирования систем управления информационной безопасностью на объекте защиты. / Лаб /	1	12	ОПК-3,УК- 3	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
2.3	Тема 1 "Информационное противоборство, методы и средства его ведения. Методы и средства обеспечения информационной безопасности объектов информационной сферы». Аудит состояния информационной безопасности на объектах информатизации. / Пр /	1	8	ОПК-3,УК- 3	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.4, Л2.5
2.4	Тема 1 "Информационное противоборство, методы и средства его ведения. Методы и средства обеспечения информационной безопасности объектов информационной сферы». Классификация возможных каналов утечки информации. Технологии зашиты акустической информации от утечки. Технологии зашиты информации от утечки по каналам ПЭМИН. Технологии зашиты видовой информации от утечки. / Ср /	1	4	ОПК-3,УК- 3	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
2.5	«Управление безопасностью в компьютерной системе». Классификация методов зашиты информации от программно-математических воздействий. Категорирование объектов информатизации. Деятельность администратора безопасности по предотвращению программно-математических воздействий. Деятельность администратора безопасности по минимизации последствий программно-математических воздействий / Лек /	1	4	ОПК-3,УК- 3	Л1.1, Л1.3, Л2.1, Л2.3
2.6	Тема 2 «Управление безопасностью в компьютерной системе». Классификация методов зашиты информации от программно-математических воздействий. Категорирование объектов информатизации. Деятельность администратора безопасности по предотвращению программно-математических воздействий. Деятельность администратора безопасности по минимизации последствий программно-математических воздействий. / Лаб /	1	12	ОПК-3,УК- 3	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
2.7	Тема 2 «Управление безопасностью в компьютерной системе». Оценка эффективности проводимых мероприятий по совершенствованию системы управления информационной безопасностью. / Пр /	1	12	ОПК-3,УК- 3	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.4, Л2.5
2.8	Тема 2 «Управление безопасностью в компьютерной системе». Термины и определения. Системы удаленного управления безопасности: в отсутствии локального объекта управления, при локальном объекте управления и удаленном управляющем объекте, при распределенном объекте управления. Модели воздействия внешнего злоумышленника на локальный сегмент компьютерной	1	10	ОПК-3,УК- 3	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5

	системы. / Ср /				
2.9	/ Экзамен /	1	36	ОПК-3,УК- 3	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5

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
Л1.1	Грушо А. А., Применко Э. А., Тимонина Е. Е.	Теоретические основы компьютерной безопасности: учеб. пособие для студентов вузов, обучающихся по спец. группы 090100 "Информ. безопасность"	М.: Академия, 2009	30
Л1.2	Ковалев Д. В., Богданова Е. А.	Информационная безопасность: учебное пособие	Ростов-на-Дону: Южный федеральный университет, 2016	https://biblioclub.ru/index.php?page=book&id=493175 неограниченный доступ для зарегистрированных пользователей
Л1.3	Шаньгин, В. Ф.	Информационная безопасность и защита информации	Саратов: Профобразование, 2019	https://www.iprbookshop.ru/87995.html неограниченный доступ для зарегистрированных пользователей

5.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л2.1	Шейдаков Н. Е., Серпенинов О. В., Тищенко Е. Н.	Физические основы защиты информации: учеб. пособие для студентов высш. учеб. заведений, обучающихся по напр. подгот. "Информ. безопасность"	М.: РИО, 2016	111
Л2.2	Рытенкова О.	Информационная безопасность: журнал	Москва: ГРОТЕК, 2013	https://biblioclub.ru/index.php?page=book&id=210607 неограниченный доступ для зарегистрированных пользователей
Л2.3	Катанова, Т. Н., Галкина, Л. С., Жданов, Р. А.	Информационная безопасность: лабораторный практикум	Пермь: Пермский государственный гуманитарно-педагогический университет, 2018	https://www.iprbookshop.ru/86357.html неограниченный доступ для зарегистрированных пользователей
Л2.4	Морозов, А. В., Филатова, Л. В., Полякова, Т. А.	Информационное право и информационная безопасность. Часть 2: учебник для магистров и аспирантов	Москва, Саратов: Всероссийский государственный университет юстиции (РПА Минюста России), Ай Пи Эр Медиа, 2016	https://www.iprbookshop.ru/66771.html неограниченный доступ для зарегистрированных пользователей
Л2.5	Морозов, А. В., Филатова, Л. В., Полякова, Т. А.	Информационное право и информационная безопасность. Часть 1: учебник для магистров и аспирантов	Москва, Саратов: Всероссийский государственный университет юстиции (РПА Минюста России), Ай Пи Эр Медиа, 2016	https://www.iprbookshop.ru/72395.html неограниченный доступ для зарегистрированных пользователей

5.3 Профессиональные базы данных и информационные справочные системы

ИСС "КонсультантПлюс"

ИСС "Гарант" http://www.internet.garant.ru/

ЭБС «IPR Books» http://www.iprbookshop.ru/
Библиоклуб.ру http://biblioclub.ru/
5.4. Перечень программного обеспечения
LibreOffice
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.

Приложение 1

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
УК-1 –способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели			
З. методики формирования команд; методы эффективного руководства коллективами.(соотнесено с индикатором УК-3.1.)	поиск и сбор необходимой литературы, использование различных баз данных	полнота и содержательность ответа умение приводить примеры	Т (тесты Раздел 1 тема 1 вопрос 1-2; Раздел 2 тема 1 вопрос 1), Э (вопросы 1-4, 9-11, 25-26)
У. разрабатывать командную стратегию; организовывать работу коллективов; управлять коллективом; разрабатывать мероприятия по личностному, образовательному и профессиональному росту(соотнесено с индикатором УК-3.2.)	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	ПЗ (Раздел 1 практическое задание 1, часть 1); ЛЗ (Раздел 1 лабораторное задание 1, часть 1) ПОЗЭ (1-5)
В. методами организации и управления коллективом, планированием его действий.(соотнесено с индикатором УК-3.3.)	использование современных информационно-коммуникационных технологий и различных информационных ресурсов	полнота и содержательность ответа умение приводить примеры умение самостоятельно находить решение поставленных задач	ПЗ (Раздел 1 практическое задание 1, часть 2); ЛЗ (Раздел 1 лабораторное задание 1, часть 2) ПОЗЭ (1-5)
ОПК-3- способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности			
З. основы отечественных и зарубежных стандартов в области сертификации и аттестации объектов информатизации, в области управления информационной безопасностью с целью разработки проектов организационно-распорядительных документов	актуальность тем исследований и ее практическая новизна	полнота и содержательность ответа умение приводить примеры	Т (тесты Раздел 1 тема 1 вопрос 3; Раздел 2 тема 1 вопрос 2-3), Э (вопросы 5-8, 16-18, 27-30)

(соотнесено с индикатором ОПК-3.1.)			
У. разрабатывать технические задания на создание подсистем обеспечения информационной безопасности.(соотнесено с индикатором ОПК-3.2.)	поиск и сбор необходимой литературы, анализ фундаментальных и прикладных проблем информационной безопасности	полнота и содержательность ответа умение приводить примеры умение самостоятельно находить решение поставленных задач	ПЗ (Раздел 2 практическое задание 1, часть 1) ЛЗ (Раздел 2 лабораторное задание 1, часть 1) ПОЗЭ (1-5)
В. навыками разработки политик безопасности различных уровней.(соотнесено с индикатором ОПК-3.3.)	использование современных информационно-коммуникационных технологий и глобальных информационных ресурсов	полнота и содержательность ответа умение приводить примеры умение самостоятельно находить решение поставленных задач	ПЗ (Раздел 2 практическое задание 1, часть 2); ЛЗ (Раздел 2 лабораторное задание 1, часть 2) ПОЗЭ (1-5)

ЛЗ – лабораторные задания, ПЗ- практические задания; Т – тест, Э – вопросы к экзамену ПОЗЭ – практико-ориентированные задания к экзамену

1.2 Шкалы оценивания:

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

84-100 баллов (оценка «отлично»)
67-83 баллов (оценка «хорошо»)
50-66 баллов (оценка «удовлетворительно»)
0-49 баллов (оценка «неудовлетворительно»)

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 экзамену

1. Обеспечение информационной безопасности при вводе объектов в эксплуатацию.
2. Специальные проверки и специальные исследования.
3. Информационная безопасность: основные определения.
4. Понятие конфиденциальности, целостности, доступности информации.
5. Формальные модели управления доступом: модель Харрисона-Руззо-Ульмана, модель Белла Ла-Падулы. Формальные модели целостности: модель Кларка-Вилсона, модель Биба.
6. Совместное использование моделей безопасности.
7. Ролевое управление доступом.

8. Выбор и оптимизация требуемых мер и средств защиты информации на объектах.
9. Аттестация объектов информатизации.
10. Контроль за обеспечением безопасной эксплуатации объектов информатизации.
11. Теоретические основы построения систем защиты от угроз».
12. Классификация угроз информационной безопасности.
13. Построение систем защиты от угроз нарушения конфиденциальности информации: модель системы защиты, организационное обеспечение ИБ, идентификация и аутентификация, разграничение доступа, криптографические методы, контроль внешнего периметра, протоколирование, аудит.
14. Построение систем защиты от угроз нарушения целостности информации: модель обеспечения целостности, криптографические методы.
15. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем.
16. Информационное противоборство, информационная война.
17. Методы нарушения конфиденциальности, целостности и доступности информации в условиях информационного противоборства.
18. Основные направления обеспечения информационной безопасности объектов информационной сферы государства в условиях информационной войны.
19. Правовые, организационно-технические и экономические методы обеспечения ИБ.
20. Модели, стратегии и системы обеспечения информационной безопасности в условиях информационного противоборства.
21. Классификация возможных каналов утечки информации.
22. Технологии зашиты акустической информации от утечки.
23. Технологии зашиты информации от утечки по каналам ПЭМИН.
24. Технологии зашиты видовой информации от утечки.
25. Классификация методов зашиты информации от программно-математических воздействий.
26. Категорирование объектов информатизации.
27. Деятельность администратора безопасности по предотвращению программно-математических воздействий.
28. Деятельность администратора безопасности по минимизации последствий программно-математических воздействий.
29. Системы удаленного управления безопасности: в отсутствии локального объекта управления, при локальном объекте управления и удаленном управляющем объекте, при распределенном объекте управления.
30. Модели воздействия внешнего злоумышленника на локальный сегмент компьютерной системы.

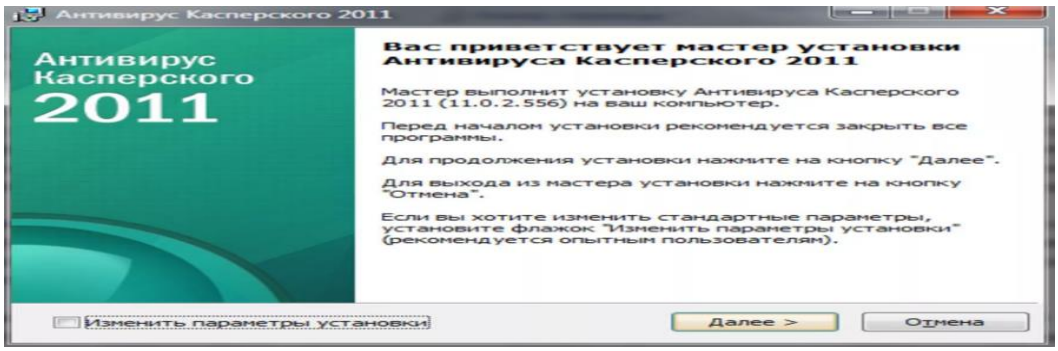
Практико-ориентированные задания к экзамену

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 антивирусное программное обеспечение:



Установить и настроить Linux-подобную операционную систему.

Установить шифровальную систему.

Критерии оценивания:

- 84-100 баллов (оценка «отлично») - изложенный материал фактически верен, наличие глубоких исчерпывающих знаний в объеме пройденной программы дисциплины в соответствии с поставленными программой курса целями и задачами обучения; правильные, уверенные действия по применению полученных знаний на практике, грамотное и логически стройное изложение материала при ответе, усвоение основной и знакомство с дополнительной литературой;

- 67-83 баллов (оценка «хорошо») - наличие твердых и достаточно полных знаний в объеме пройденной программы дисциплины в соответствии с целями обучения, правильные действия по применению знаний на практике, четкое изложение материала, допускаются отдельные логические и стилистические погрешности; усвоена основная литература, рекомендованная в рабочей программе дисциплины;

- 50-66 баллов (оценка «удовлетворительно») - наличие твердых знаний в объеме пройденного курса в соответствии с целями обучения, изложение ответов с отдельными ошибками, уверенно исправленными после дополнительных вопросов; выполняются в целом корректные действия по применению знаний на практике;

- 0-49 баллов (оценка «неудовлетворительно») - ответы не связаны с вопросами, наличие грубых ошибок в ответе, демонстрирующие непонимание сущности излагаемого вопроса и неумение применять знания на практике; отсутствие уверенности и неточность ответов на дополнительные и наводящие вопросы.

Тесты

Раздел 1 Системы управления информационной безопасности

Тема 1 " Основные положения теории информационной безопасности "

1. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?

а) сотрудники

б) хакеры

в) атакующие

г) контрагенты (лица, работающие по договору)

2. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?

а) владельцы данных

б) пользователи

в) администраторы

г) руководство

3. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?

а) поддержка высшего руководства

б) эффективные защитные меры и методы их внедрения

в) актуальные и адекватные политики и процедуры безопасности

г) проведение тренингов по безопасности для всех сотрудников

Тема 2 " Угрозы информационной безопасности. Теоретические основы построения систем защиты от угроз».

1. Что такое политики безопасности?

а) инструкции по выполнению задач безопасности

б) общие руководящие требования по достижению определенного уровня безопасности

в) широкие, высокоуровневые заявления руководства

г) детализированные документы по обработке инцидентов безопасности

2. Какая из приведенных техник является самой важной при выборе конкретных защитных мер?

а) анализ рисков

б) анализ затрат / выгоды

в) результаты ALE

г) выявление уязвимостей и угроз, являющихся причиной риска

3. Какая из приведенных техник является самой важной при выборе конкретных защитных мер?

а) анализ рисков

б) анализ затрат / выгоды

в) результаты ALE

г) выявление уязвимостей и угроз, являющихся причиной риска

Раздел 2. Методы и технологии информационной безопасности

Тема 1. «Информационное противоборство, методы и средства его ведения. Методы и средства обеспечения информационной безопасности объектов информационной сферы».

1. 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

2. Эффективная программа безопасности требует сбалансированного применения:

а) технических и нетехнических методов

б) контрмер и защитных механизмов

в) физической безопасности и технических средств защиты

г) процедур безопасности и шифрования

3. Что из перечисленного не является целью проведения анализа рисков?

а) делегирование полномочий

б) количественная оценка воздействия потенциальных угроз

в) выявление рисков

г) определение баланса между воздействием риска и стоимостью необходимых контрмер

Тема 2. «Управление безопасностью в компьютерной системе».

1.Что из перечисленного не является задачей руководства в процессе внедрения и сопровождения безопасности?

а) поддержка

б) выполнение анализа рисков

в) определение цели и границ

г) делегирование полномочий

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

a) да

b) нет

3.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.

3. Критерии оценки:

- 1-20 баллов выставляется обучаемому. За один правильный ответ обучаемый получает 2 балла.

Лабораторные задания

1.Тематика лабораторных заданий по разделам и темам

Раздел 1 «**Системы управления информационной безопасности**»

Тема 1 «Основные положения теории информационной безопасности»

Лабораторная работа 1 Исследование архитектуры построения систем управления информационной безопасностью. Оформление при помощи LibreOffice.

Тема 2 «Угрозы информационной безопасности. Теоретические основы построения систем защиты от угроз».

Лабораторная работа 2. Теоретические основы построения систем защиты от угроз». Исследование свойств локальной политики безопасности. Оформление при помощи LibreOffice.

Раздел 2. «**Методы и технологии информационной безопасности**».

Тема 1. «Информационное противоборство, методы и средства его ведения. Методы и средства обеспечения информационной безопасности объектов информационной сферы».

Лабораторная работа 1. Исследование функционирования систем управления информационной безопасностью на объекте защиты.

Тема 2. «Управление безопасностью в компьютерной системе».

Лабораторная работа 2. Классификация методов зашиты информации от программно-математических воздействий. Категорирование объектов информатизации. Деятельность администратора безопасности по предотвращению программно-математических воздействий. Деятельность администратора безопасности по минимизации последствий программно-математических воздействий.

Критерии оценки:

- (для каждого задания):

10 б. – задание выполнено верно;

9-7 б. – при выполнении задания были допущены неточности, не влияющие на результат;

6-3 б. – при выполнении задания были допущены ошибки;

2 - 1 б. – при выполнении задания были допущены существенные ошибки;

0 б. – задание не выполнено.

Практические задания

1.Тематика практических заданий по разделам и темам

Раздел 1 «**Системы управления информационной безопасности**»

Тема 1 «Основные положения теории информационной безопасности»

Практическое занятие 1 Управление информационной безопасностью объекта информатизации.

Тема 2 «Угрозы информационной безопасности. Теоретические основы построения систем защиты от угроз».

Практическое занятие 2. Управление средствами защиты информации на объекте.

Раздел 2. «**Методы и технологии информационной безопасности**».

Тема 1. «Информационное противоборство, методы и средства его ведения. Методы и средства обеспечения информационной безопасности объектов информационной сферы».

Практическое занятие 1. Аудит состояния информационной безопасности на объектах информатизации.

Тема 2. «Управление безопасностью в компьютерной системе».

Практическое занятие 2. Оценка эффективности проводимых мероприятий по совершенствованию системы управления информационной безопасностью.

2. Критерии оценки:

10 б. – задание выполнено верно;
9-7 б. – при выполнении задания были допущены неточности, не влияющие на результат;
6-3 б. – при выполнении задания были допущены ошибки;
2 - 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.

Экзамен проводится по расписанию п**ромежуточной аттестации**.

Экзамен проводится по расписанию промежуточной аттестации в письменном виде. Количество вопросов в экзаменационном задании – 3. Проверка ответов и объявление результатов производится в день экзамена. Результаты аттестации заносятся в экзаменационную ведомость и зачетную книжку студента. Студенты, не прошедшие промежуточную аттестацию по графику сессии, должны ликвидировать задолженность в установленном порядке.

Приложение 2

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Учебным планом предусмотрены следующие виды занятий:

- лекции;
- практические занятия;
- лабораторные занятия.

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

При подготовке к практическим занятиям каждый студент должен:

– изучить рекомендованную учебную литературу;

– подготовить ответы на все вопросы по изучаемой теме;

–письменно решить домашнее задание, рекомендованные преподавателем при изучении каждой темы.

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

Вопросы, не рассмотренные на практических занятиях, должны быть изучены студентами в ходе самостоятельной работы. Контроль самостоятельной работы студентов над учебной программой курса осуществляется в ходе занятий методом устного опроса или посредством тестирования. В ходе самостоятельной работы каждый студент обязан прочитать основную и по возможности дополнительную литературу по изучаемой теме. Выделить непонятные термины, найти их значение в энциклопедических словарях.

Студент должен готовиться к предстоящему лабораторному занятию по всем, обозначенным в рабочей программе дисциплины вопросам.

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.