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
Технологии выявления следов компьютерных преступлений, правонарушений и инцидентов

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>)	4 (2.2)		Итого	
Недель	7 4/6			
Вид занятий	УП	РП	УП	РП
Лекции	10	10	10	10
Лабораторные	20	20	20	20
Практические	20	20	20	20
Итого ауд.	50	50	50	50
Контактная работа	50	50	50	50
Сам. работа	85	85	85	85
Часы на контроль	9	9	9	9
Итого	144	144	144	144

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.т.н., профессор, Тищенко Е.Н. _____

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1	дать представление об основных типах технических и программных средств, используемых для выявления следов компьютерных преступлений,получить навыки по использованию современного инструментария предназначенного для построения современных комплексных систем защиты информации объекта информатизации.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

УК-1:Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий

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:

принципы построения и организацию функционирования современных устройств и систем хранения, обработки, поиска и передачи информации (соотнесено с индикатором УК-1.1);
основные принципами использования программно-аппаратных комплексов защиты информации объекта информатизации (соотнесено с индикатором ПК-4.1).

Уметь:

Сравнивать технико-эксплуатационные возможности устройств и систем защиты информации объекта информатизации, расшифровывать и анализировать информацию о параметрах и характеристиках устройств и систем защиты информации объекта информатизации с использованием различных источников (соотнесено с индикатором УК-1.2);
Устанавливать, настраивать, использовать программно-аппаратные средства защиты информации объекта информатизации (соотнесено с индикатором ПК-4.2).

Владеть:

Навыками расшифровки и анализа информации о параметрах и характеристиках устройств и систем защиты информации объекта информатизации с использованием различных источников (соотнесено с индикатором УК-1.3)
Установкой, настройкой программно - аппаратных средства защиты информации объекта информатизации (соотнесено с индикатором ПК-4.3).

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература
	Раздел 1. Технологии выявления компьютерных преступлений				
1.1	"Цель, задачи, содержание и структура дисциплины":место дисциплины в системе подготовки специалистов по защите информации. /Лек/	4	2	УК-1 ПК-4	Л1.1Л2.1
1.2	"Цель, задачи, содержание и структура дисциплины":место дисциплины в системе подготовки специалистов по защите информации. /Пр/	4	2	УК-1 ПК-4	Л1.1 Л1.2Л2.1 Л2.2
1.3	"Цель, задачи, содержание и структура дисциплины":место дисциплины в системе подготовки специалистов по защите информации. /Ср/	4	6	УК-1 ПК-4	Л1.1 Л1.2Л2.1 Л2.2 Л2.3
1.4	"Концепция создания защищенных информационно-телекоммуникационных систем":основные требования и принципы создания защищенных информационно-телекоммуникационных систем /Лаб/	4	4	УК-1 ПК-4	Л1.1Л2.1 Л2.2 Л2.3
1.5	"Концепция создания защищенных информационно-телекоммуникационных систем":основные требования и принципы создания защищенных информационно-телекоммуникационных систем /Пр/	4	2	УК-1 ПК-4	Л1.1 Л1.2Л2.1 Л2.2
1.6	"Концепция создания защищенных информационно-телекоммуникационных систем":основные требования и принципы создания защищенных информационно-телекоммуникационных систем /Ср/	4	10	УК-1 ПК-4	Л1.1 Л1.2Л2.1 Л2.2 Л2.3

1.7	"Этапы создания комплексной системы защиты информации":основные этапы создания комплексной системы защиты информации и их характеристика. /Лаб/	4	4	УК-1 ПК-4	Л1.1 Л1.2Л2.1 Л2.2
1.8	"Этапы создания комплексной системы защиты информации":основные этапы создания комплексной системы защиты информации и их характеристика. /Пр/	4	2	УК-1 ПК-4	Л1.1 Л1.2Л2.1 Л2.2 Л2.3
1.9	"Этапы создания комплексной системы защиты информации":основные этапы создания комплексной системы защиты информации и их характеристика. /Ср/	4	6	УК-1 ПК-4	Л1.1 Л1.2Л2.1 Л2.2 Л2.3
1.10	"Научно-исследовательская разработка КСЗИ":принципы и этапы научно-исследовательских разработок КСЗИ. /Лаб/	4	2	УК-1 ПК-4	Л1.1 Л1.2Л2.1
1.11	"Научно-исследовательская разработка КСЗИ":принципы и этапы научно-исследовательских разработок КСЗИ. /Лек/	4	2	УК-1 ПК-4	Л1.1 Л1.2Л2.2 Л2.3
1.12	"Научно-исследовательская разработка КСЗИ":принципы и этапы научно-исследовательских разработок КСЗИ. /Ср/	4	10	УК-1 ПК-4	Л1.1 Л1.2Л2.1 Л2.2
1.13	"Моделирование КСЗИ": классификация и характеристика различных типом моделей, используемых при создании КСЗИ. /Лаб/	4	4	УК-1 ПК-4	Л1.1 Л1.2Л2.1 Л2.2 Л2.3
1.14	"Моделирование КСЗИ": классификация и характеристика различных типом моделей, используемых при создании КСЗИ. /Пр/	4	2	УК-1 ПК-4	Л1.1 Л1.2Л2.2 Л2.3
1.15	"Моделирование КСЗИ": классификация и характеристика различных типом моделей, используемых при создании КСЗИ. /Ср/	4	10	УК-1 ПК-4	Л1.1 Л1.2Л2.1 Л2.2
1.16	"Специальные методы неформального моделирования": содержание и характеристика специальных методов неформального моделирования; метод экспертного оценивания. /Лаб/	4	2	УК-1 ПК-4	Л1.1 Л1.2Л2.1 Л2.2
1.17	"Специальные методы неформального моделирования": содержание и характеристика специальных методов неформального моделирования; метод экспертного оценивания. /Ср/	4	2	УК-1 ПК-4	Л1.1 Л1.2Л2.1 Л2.2
1.18	Классификация информационных систем и категорирование объекта информатизациии. /Пр/	4	2	УК-1 ПК-4	Л1.1 Л1.2Л2.1 Л2.2
1.19	Классификация информационных систем и категорирование объекта информатизациии. /Ср/	4	9	УК-1 ПК-4	Л1.1 Л1.2Л2.1 Л2.3
1.20	"Применение КСЗИ по назначению":особенности применения КСЗИ при организации защиты информации на объектах информатизации. /Лаб/	4	2	УК-1 ПК-4	Л1.1 Л1.2Л2.1
1.21	"Применение КСЗИ по назначению":особенности применения КСЗИ при организации защиты информации на объектах информатизации. /Ср/	4	6	УК-1 ПК-4	Л1.1 Л1.2Л2.2
1.22	"Применение КСЗИ по назначению":особенности применения КСЗИ при организации защиты информации на объектах информатизации. /Ср/	4	2	УК-1 ПК-4	Л1.1 Л1.2Л2.1 Л2.3
	Раздел 2. Комплексных систем защиты информации				
2.1	"Техническая эксплуатация КСЗИ":основные этапы эксплуатации КСЗИ; требования при эксплуатации КСЗИ. /Лек/	4	2	УК-1 ПК-4	Л1.1 Л1.2Л2.1 Л2.2
2.2	"Техническая эксплуатация КСЗИ":основные этапы эксплуатации КСЗИ; требования при эксплуатации КСЗИ. /Пр/	4	2	УК-1 ПК-4	Л1.1 Л1.2Л2.2 Л2.3
2.3	"Техническая эксплуатация КСЗИ":основные этапы эксплуатации КСЗИ; требования при эксплуатации КСЗИ. /Ср/	4	6	УК-1 ПК-4	Л1.1 Л1.2Л2.1 Л2.2 Л2.3

2.4	"Планирование эксплуатации КСЗИ":цели планирования;виды планирования и их назначение;методы и формы контроля выполнения планов. /Лаб/	4	2	УК-1 ПК-4	Л1.1 Л1.2Л2.1 Л2.2
2.5	"Планирование эксплуатации КСЗИ":цели планирования;виды планирования и их назначение;методы и формы контроля выполнения планов. /Пр/	4	4	УК-1 ПК-4	Л1.1 Л1.2Л2.2
2.6	"Планирование эксплуатации КСЗИ":цели планирования;виды планирования и их назначение;методы и формы контроля выполнения планов. /Ср/	4	6	УК-1 ПК-4	Л1.1 Л1.2Л2.1 Л2.3
2.7	"Управление комплексной системой защиты информации в условиях чрезвычайных ситуаций";особенности управление комплексной системой защиты информации в условиях чрезвычайных ситуаций. /Лек/	4	4	УК-1 ПК-4	Л1.1 Л1.2Л2.1 Л2.2 Л2.3
2.8	"Управление комплексной системой защиты информации в условиях чрезвычайных ситуаций";особенности управление комплексной системой защиты информации в условиях чрезвычайных ситуаций. /Пр/	4	2	УК-1 ПК-4	Л1.1 Л1.2Л2.1 Л2.2 Л2.3
2.9	"Управление комплексной системой защиты информации в условиях чрезвычайных ситуаций";особенности управление комплексной системой защиты информации в условиях чрезвычайных ситуаций. /Ср/	4	6	УК-1 ПК-4	Л1.1 Л1.2Л2.1 Л2.2
2.10	Анализ и использование результатов проведения контрольных мероприятий функционирования КСЗИ. /Пр/	4	2	УК-1 ПК-4	Л1.1 Л1.2Л2.1 Л2.2
2.11	Анализ и использование результатов проведения контрольных мероприятий функционирования КСЗИ. /Ср/	4	6	УК-1 ПК-4	Л1.1 Л1.2Л2.1 Л2.2 Л2.3
2.12	/Экзамен/	4	9	УК-1 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
Л1.1	Сердюк В. А.	Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий: учебное пособие	Москва: Издательский дом Высшей школы экономики, 2015	http://biblioclub.ru/index.php?page=book&id=440285 неограниченный доступ для зарегистрированных пользователей
Л1.2	Фомичев, В. М.	Сборник задач по криптологии: сборник задач для студентов, обучающихся по направлению: 10.03.01 «информационная безопасность», профиль: «комплексная защита объектов информации»	Москва: Прометей, 2019	http://www.iprbookshop.ru/94524.html неограниченный доступ для зарегистрированных пользователей

5.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Колич-во

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л2.1		Комплексное обеспечение информационной безопасности автоматизированных систем: лабораторный практикум: практикум	Ставрополь: Северо-Кавказский Федеральный университет (СКФУ), 2016	https://biblioclub.ru/index.php?page=book&id=458012 неограниченный доступ для зарегистрированных пользователей
Л2.2	Фомин, Д. В.	Информационная безопасность: учебно-методическое пособие по дисциплине «информационная безопасность» для студентов экономических специальностей заочной формы обучения	Саратов: Вузовское образование, 2018	http://www.iprbookshop.ru/77320.html неограниченный доступ для зарегистрированных пользователей
Л2.3		БИТ. Бизнес & Информационные технологии: журнал	Москва: Положевец и партнеры, 2018	https://biblioclub.ru/index.php?page=book&id=562398 неограниченный доступ для зарегистрированных пользователей

5.3 Профессиональные базы данных и информационные справочные системы

ConsultantPlus

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 осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий			
З. принципы построения и организацию функционирования современных устройств и систем хранения, обработки, поиска и передачи информации (соотнесено с индикатором УК-1.1)	Угрозы безопасности информации. Система защиты информации. Законодательно - правовые и организационные основы обеспечения защиты информации.	полнота и содержательность ответа умение приводить примеры	Э(1 – 20). О (1-20)
У. Сравнивать технико-эксплуатационные возможности устройств и систем защиты информации объекта информатизации, расшифровывать и анализировать информацию о параметрах и характеристиках устройств и систем защиты информации объекта информатизации с использованием различных источников (соотнесено с индикатором УК-1.2)	Организация защиты информации на предприятии. Политика безопасности предприятия. Структура системы государственного лицензирования.	полнота и содержательность ответа умение приводить примеры умение самостоятельно находить решение поставленных задач	ЛЗ (1-6) ПЗ (1-3) ПОЗЭ(1-5)
В. Навыками расшифровки и анализа информации о параметрах и характеристиках устройств и систем защиты информации объекта информатизации с использованием различных источников (соотнесено с индикатором УК-1.3)	Порядок проведения администрирования подсистемы информационной безопасности объекта защиты.	полнота и содержательность ответа умение приводить примеры умение самостоятельно находить решение поставленных задач	ЛЗ (1-6) ПЗ (1-3) ПОЗЭ (1-5)
ПК-4 – способен осуществлять анализ результатов экспериментальных исследований с применением математических и физических методов, выбор технических средств инструментального мониторинга защищенности объетов			
З. основные принципами использования программно-аппаратных комплексов защиты информации объекта информатизации (соотнесено с индикатором ПК-4.1)	Объекты защиты. Направления, методы и перечень видов деятельности при реализации комплексной защиты информации.	полнота и содержательность ответа умение приводить примеры	Э (20-30) О(20-30)

У. Устанавливать, настраивать, использовать программно-аппаратные средства защиты информации объекта информатизации (соотнесено с индикатором ПК-4.2)	Организация защиты информации на предприятии. Политика безопасности предприятия. Организационные и технические способы защиты информаци. Организационное управление защитой информации.	полнота и содержательность ответа умение приводить примеры умение самостоятельно находить решение поставленных задач	ЛЗ (1-6) ПЗ (1-3) ПОЗЭ (1-5)
В. Установкой, настройкой программно - аппаратных средства защиты информации объекта информатизации (соотнесено с индикатором ПК-4.3)	Перечень сведений конфиденциального характера. Мероприятия по защите конфиденциальной информации. Полномочия органов государственной власти и должностных лиц.	полнота и содержательность ответа умение приводить примеры умение самостоятельно находить решение поставленных задач	ЛЗ (1-6) ПЗ (1-3) ПОЗЭ (1-5)

ЛЗ- лабораторные задания, ПЗ – практические задания, Э– вопросы к экзамену, О –опрос ПОЗЭ- практико-ориентированные задания к экзамену

1.2 Шкалы оценивания:

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. Понятие и сущность КСЗИ.
2. Назначение КСЗИ.
3. КСЗИ как средство выражения концептуальных основ защиты информации.
4. Методологические основы организации КСЗИ.
5. Основные положения теории систем.
6. Характер и степень влияния различных факторов на организацию КСЗИ.
7. Методика определения состава защищаемой информации.
8. Работы по выявлению состава защищаемой информации.
9. Значение носителей защищаемой информации как объектов защиты.
10. Методика выявления состава носителей защищаемой информации.
11. Определение источников дестабилизирующего воздействия на информацию и видов их воздействия.
12. Методика выявления способов воздействия на информацию.
13. Методика выявления каналов несанкционированного доступа к информации.
14. Оценка степени целостности информации в результате действий нарушителей различных категорий.
15. Факторы, влияющие на выбор компонентов КСЗИ.
16. Основные требования, предъявляемые к выбору методов и средств защиты.
17. Понятие модели объекта, основные виды моделей и их характеристика.
18. Характеристика основных стадий создания КСЗИ.
19. Определение состава кадрового обеспечения функционирования КСЗИ.
20. Определение состава материально-технического обеспечения, его зависимость от структуры КСЗИ.

21. Понятие и цели управления КСЗИ. Сущность процессов управления КСЗИ.
22. Понятие и задачи планирования функционирования КСЗИ. Способы и методы планирования.
23. Понятие и виды контроля функционирования КСЗИ. Цель проведения контрольных мероприятий в КСЗИ. Методы контроля.
24. Понятие и основные виды чрезвычайных ситуаций. Технология принятия решений в условиях чрезвычайной ситуации.
25. Классификация подходов к оценке эффективности систем защиты информации.
26. Оценочный подход на основе формирования требований к защищенности объекта.
27. Сравнительный анализ подходов оценки эффективности систем защиты информации.
28. Классификационная структура методов и моделей оценки эффективности комплексной системы защиты информации.
29. Системы показателей защищенности (эффективности).
30. Метод оценки эффективности на основе структурных вопросников.

Типовые практико-ориентированные задания к экзамену

Задание 1. Добавить пользователей в компьютер.
Задание 2. Создать учетную запись локального пользователя.
Задание 3. Измените учетную запись локального пользователя на учетную запись администратора.
Задание 4.Выполнить настройку учетной записи с ограниченными правами.
Задание 5. Выполнить добавление учетных записей, используемых приложениями.

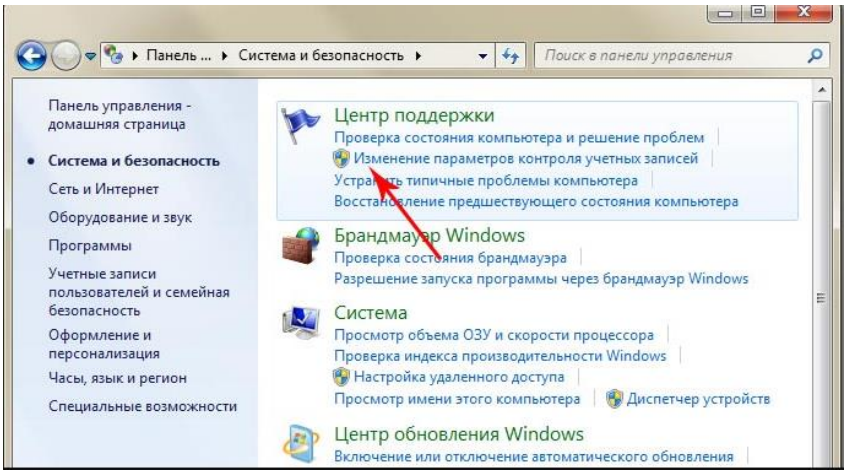
Ключ для контроля правильности выполнения практико-ориентированные задания к зачету

1. Добавление пользователей в рабочий или учебный компьютер. Выберите параметры > "Пуск" > " Учетные записи > Другие пользователи". В разделе "Рабочие или учебные > добавить рабочую или учебную учетную запись" выберите " Добавить учетную запись". Введите учетную запись этого пользователя, выберите тип учетной записи и нажмите Добавить.

2. Создание учетной записи локального пользователя. Выберите Пуск > Параметры > Учетные записи, а затем Семья и другие пользователи. Рядом с пунктом Добавить другого пользователя выберите Добавить учетную запись. Выберите пункт У меня нет учетных данных этого пользователя и на следующей странице нажмите Добавить пользователя без учетной записи Майкрософт. Введите имя пользователя, пароль, подсказку о пароле или выберите секретные вопросы, а затем нажмите Далее.

3. Изменение учетной записи локального пользователя на учетную запись администратора. Выберите Пуск > Параметры > Учетные записи. В разделе Семья и другие пользователи щелкните имя владельца учетной записи (под ним должно быть указано "Локальная учетная запись") и выберите Изменить тип учетной записи. В разделе Тип учетной записи выберите Администратор, и нажмите ОК. Войдите в систему с новой учетной записью администратора.

4.



5.Добавление на компьютер учетной записи, используемой приложениями: Выберите **параметры >** параметров **> учетных** записей **> электронной почты & учетных записей**. Добавление учетной записи, используемой по электронной почте. выберите "Добавить учетную запись" в разделе "Учетные записи", используемые электронной почтой**, календарем и** контактами. Для других приложений выберите "Добавить учетную запись Майкрософт " или "Добавить рабочую или учебную учетную

запись". Следуйте инструкциям по добавлению учетной записи.

Критерии оценивания:

- оценка «отлично» (84-100 баллов) выставляется, если 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;
- оценка хорошо» (67-83 баллов) – 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, студент усвоил основную литературу, рекомендованную в рабочей программе дисциплины;
- оценка «удовлетворительно» (50-66 баллов) – наличие твердых знаний в объеме пройденного курса в соответствии с целями обучения, изложение ответов с отдельными ошибками, уверенно исправленными после дополнительных вопросов; правильные в целом действия по применению знаний на практике;
- оценка неудовлетворительно» (0-49 баллов) ответы не связаны с вопросами, наличие грубых ошибок в ответе, непонимание сущности излагаемого вопроса, неумение применять знания на практике, неуверенность и неточность ответов на дополнительные и наводящие вопросы».

Лабораторные задания

1. "Концепция создания защищенных информационно-телекоммуникационных систем":основные требования и принципы создания защищенных информационно- телекоммуникационных систем

2. "Этапы создания комплексной системы защиты информации":основные этапы создания комплексной системы защиты информации и их характеристика.

3. "Научно-исследовательская разработка КСЗИ":принципы и этапы научно-исследовательских разработок КСЗИ.

4. "Моделирование КСЗИ": классификация и характеристика различных типом моделей, используемых при создании КСЗИ.

5. "Специальные методы неформального моделирования": содержание и характеристика специальных методов неформального моделирования; метод экспертного оценивания.

6. "Применение КСЗИ по назначению":особенности применения КСЗИ при организации защиты информации на объектах информатизации.

Критерии оценки к каждому заданию:
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. "Техническая эксплуатация КСЗИ":основные этапы эксплуатации КСЗИ; требования при эксплуатации КСЗИ.

2. "Планирование эксплуатации КСЗИ":цели планирования;виды планирования и их назначение;методы и формы контроля выполнения планов.

3. "Управление комплексной системой защиты информации в условиях чрезвычайных ситуаций";особенности управление комплексной системой защиты информации в условиях чрезвычайных ситуаций.

Критерии оценки к каждому заданию:
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.

Вопросы для опроса

1. Понятие и сущность КСЗИ.
2. Назначение КСЗИ.
3. КСЗИ как средство выражения концептуальных основ защиты информации.
4. Методологические основы организации КСЗИ.
5. Основные положения теории систем.
6. Характер и степень влияния различных факторов на организацию КСЗИ.
7. Методика определения состава защищаемой информации.
8. Работы по выявлению состава защищаемой информации.
9. Значение носителей защищаемой информации как объектов защиты.
10. Методика выявления состава носителей защищаемой информации.
11. Определение источников дестабилизирующего воздействия на информацию и видов их воздействия.
12. Методика выявления способов воздействия на информацию.
13. Методика выявления каналов несанкционированного доступа к информации.
14. Оценка степени целостности информации в результате действий нарушителей различных категорий.
15. Факторы, влияющие на выбор компонентов КСЗИ.
16. Основные требования, предъявляемые к выбору методов и средств защиты.
17. Понятие модели объекта, основные виды моделей и их характеристика.
18. Характеристика основных стадий создания КСЗИ.
19. Определение состава кадрового обеспечения функционирования КСЗИ.
20. Определение состава материально-технического обеспечения, его зависимость от структуры КСЗИ.
21. Понятие и цели управления КСЗИ. Сущность процессов управления КСЗИ.
22. Понятие и задачи планирования функционирования КСЗИ. Способы и методы планирования.
23. Понятие и виды контроля функционирования КСЗИ. Цель проведения контрольных мероприятий в КСЗИ. Методы контроля.
24. Понятие и основные виды чрезвычайных ситуаций. Технология принятия решений в условиях чрезвычайной ситуации.
25. Классификация подходов к оценке эффективности систем защиты информации.
26. Оценочный подход на основе формирования требований к защищенности объекта.
27. Сравнительный анализ подходов оценки эффективности систем защиты информации.
28. Классификационная структура методов и моделей оценки эффективности комплексной системы защиты информации.
29. Системы показателей защищенности (эффективности).
30. Метод оценки эффективности на основе структурных вопросников.

Критерии оценивания:

Для каждого вопроса:

- 1 балл дан полный ответ на поставленный вопрос, изложение материала при ответе – грамотное и логически стройное;
- 0 баллов – обучающийся не владеет материалом по заданному вопросу.

Максимальное количество баллов – 10

3. Методические материалы, определяющие процедуры оценивания результатов освоения образовательной программы

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**ромежуточная аттестация**.

В билете два вопроса: один теоретический и один практико-ориентированный. 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.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Учебным планом предусмотрены следующие виды занятий:

- лекции;
- лабораторные занятия;
- практические занятия.

В ходе лекционных занятий рассматриваются основные теоретические вопросы по дисциплине.

При подготовке к практическим и лабораторным занятиям каждый студент должен:

– изучить рекомендованную учебную литературу;

– подготовить ответы на все вопросы по изучаемой теме;

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

Вопросы, не рассмотренные на аудиторных 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 контрольной работы. В ходе самостоятельной работы каждый студент обязан прочитать основную и по возможности дополнительную литературу по изучаемой теме, дополнить конспекты недостающим материалом, выписками из рекомендованных первоисточников. Выделить непонятные термины, найти их значение в энциклопедических словарях.

Студент должен готовиться к предстоящим практическим и лабораторным занятиям 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 вузовской библиотеки или воспользоваться читальными залами вуза.