ГОУ ВПО «ДОНЕЦКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ»

ФИЗИКО-ТЕХНИЧЕСКИЙ ФАКУЛЬТЕТ

КАФЕДРА РАДИОФИЗИКИ И ИНФОКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

УТВЕРЖДАЮ:
проректор по научно-методической и учебной работе
_____ Е.И. Скафа
«23» апреля 2020 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ «ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИЕ СИСТЕМЫ БЕЗОПАСНОСТИ»

Направление подготовки:	10.04.01 Информационная безопасность
Магистерская программа:	Информационная безопасность
Образовательная программа:	академическая магистратура
Квалификация:	магистр
Форма обучения:	очная

Донецк 2020

УТВЕРЖДАЮ:
Декан физико-технического
факультета
_____ С. А. Фоменко
«17» апреля 2020 г.

МП

Программа составлена с учетом Федерального государственного образовательного стандарта высшего образования направления подготовки 10.04.01 Информационная безопасность, утвержденного приказом Министерства образования и науки Российской Федерации от 01 декабря 2016г. № 1513;
учебного плана и основной образовательной программы Информационная безопасность направления подготовки 10.04.01 Информационная безопасность разработанных в ГОУ ВПО «Донецкий национальный университет».

Разработчик:
к.т.н., доцент кафедры радиофизики
и инфокоммуникационных технологий _____ О.Г. Шелехова

Программа учебной дисциплины утверждена на заседании кафедры радиофизики и инфокоммуникационных технологий
Протокол №17 от «06» апреля 2020 г.

Заведующий кафедрой радиофизики
и инфокоммуникационных технологий _____ Данилов В.В.

Программа учебной дисциплины одобрена учебно-методической комиссией физико-технического факультета
Протокол №5 от «15» апреля 2020 г.

Председатель учебно-методической
комиссии факультета _____ В.Н. Котенко

1. ОБЛАСТЬ ПРИМЕНЕНИЯ И МЕСТО ДИСЦИПЛИНЫ В УЧЕБНОМ ПРОЦЕССЕ

Учебная дисциплина «Информационно-аналитические системы безопасности объектов» относится к базовой части профессионального блока.

Для изучения данной учебной дисциплины необходимы знания, умения и навыки, сформированные при изучении предшествующих дисциплин «Информационные технологии», «Вычислительная математика», «Электротехника», «Основы информационной безопасности», «Пакеты прикладных программ для научных расчетов», «Моделирование и системы принятия решений».

Знания, умения и навыки, усвоенные и сформированные при изучении данной учебной дисциплины, являются базовыми для и последующего изучения дисциплин: «Управление информационной безопасностью», а также других дисциплин профессионального цикла.

2. СТРУКТУРА ДИСЦИПЛИНЫ

Характеристика учебной дисциплины		
Направление подготовки	10.04.01 Информационная безопасность	
Магистерская программа	Информационная безопасность	
Программа подготовки	Академическая магистратура	
Квалификация	Магистр	
Количество содержательных модулей	2	
Дисциплина базовой / вариативной части образовательной программы	Профессиональный блок, базовая часть	
Формы контроля	Модульный контроль, сдача лабораторных работ, контрольное тестирование, дифференцированный зачет	
Показатели	очная форма обучения	заочная форма обучения
Количество зачетных единиц (кредитов)	3	
Год подготовки	1	
Семестр	1	
Количество часов	108	
- лекционных	18	
- практических, семинарских		
- лабораторных	18	
- самостоятельной работы	72	
в т.ч. индивидуальное задание		
Недельное количество часов,	5	
в т.ч. аудиторных	1	

3. ОПИСАНИЕ ДИСЦИПЛИНЫ

Цели и задачи

Цель – овладение знаниями и практическими навыками в области информационно-аналитического обеспечения информационной безопасности.

Задачи – освоение методов создания и эксплуатации современных информационно-аналитических систем безопасности; изучение подходов к построению комплексной системы информационной безопасности.

Требования к результатам освоения дисциплины. Процесс изучения дисциплины «Информационно-аналитические системы безопасности объектов» направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВО РФ по направлению подготовки 10.04.01 Информационная безопасность и основной образовательной программы высшего профессионального образования направления подготовки 10.04.01 Информационная безопасность:

а) ***общекультурных (ОК):***

способность к абстрактному мышлению, анализу, синтезу (ОК - 1);

способность самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения (ОК - 2);

способностью самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения, в том числе в новых областях знаний, непосредственно не связанных со сферой деятельности (ОК - 6).

б) ***общепрофессиональных (ОПК):***

способность к коммуникации в устной и письменной формах на государственном и одном из иностранных языков для решения задач профессиональной деятельности (ОПК-1);

способность к самостоятельному обучению и применению новых методов исследования профессиональной деятельности (ОПК-2).

в) профессиональных (ПК):

проектная деятельность

способность анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты (ПК-1);

способность разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности (ПК-2);

способность проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов (ПК-3);

способность разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности (ПК-4);

научно-исследовательская деятельность:

способность анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества (ПК-5);

способность осуществлять сбор, обработку, анализ и систематизацию научно-технической информации по теме исследования, выбор методов и средств решения задачи, разрабатывать планы и программы проведения научных исследований и технических разработок (ПК-6);

способность проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента (ПК-7);

способность обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи (ПК-8);

организационно-управленческая деятельность:

способность организовать выполнение работ, управлять коллективом исполнителей и принимать управленческие решения (ПК-12);

способность организовать управление информационной безопасностью (ПК-13);

способность организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России (ПК-14);

способность организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности (ПК-15);

способность разрабатывать проекты организационно- распорядительных документов, бизнес- планов в сфере профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности (ПК-16);

В результате изучения учебной дисциплины студент должен:

Знать:

- современные технологии проведения аналитической работы по исследованию информационной безопасности;
- отечественные и международные стандарты в области информационной безопасности;
- правовые нормативные акты и нормативные методические документы МГБ Донецкой Народной Республики;

Уметь:

- анализировать тенденции развития информационно-аналитических систем обеспечения безопасности;
- формировать функциональные требования к информационно-аналитической системе безопасности;
- определять рациональные способы и средства защиты на объекте информатизации с учетом затрат на них;

Владеть:

- навыками разработки политики информационной безопасности использование информационно-аналитических систем;
- навыками разработки структуры информационно-аналитической системы безопасности;
- навыками организации мероприятий поз защите информации на объекте в соответствие с нормативной правовой базой.

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ И ФОРМЫ ОРГАНИЗАЦИИ УЧЕБНОГО ПРОЦЕССА

Курс дисциплины «Информационно-аналитические системы безопасности объектов» предусматривает следующие *формы организации учебного процесса*:

1) лекции,
2) лабораторные занятия,
3) самостоятельная работа студента.

Порядковый номер и тема	**Краткое содержание темы**
	Содержательный модуль 1
Тема 1. Сущность, структура и задачи аналитики СБ.	Понятие и сущность аналитики системы безопасности Структура и задачи аналитики систем безопасности. Информационно-аналитические технологии системы безопасности, их задачи. Задачи и определения информационно-аналитического (ИА) обеспечения СБ, Организационные формы субъектов ИА работы;
Тема 2. Стандарты обеспечения информационной безопасности	Формирование концепций правового регулирования информационной безопасности за рубежом и в России. Системность подхода к построению стратегии кибербезопасности в США Национальные стратегии кибербезопасности в странах ЕС и НАТО. Сравнительный анализ правового обеспечения информационной безопасности в России и за рубежом Стратегия формирования правовых методов информационной безопасности Российской федерации
Тема 3. Правовые методы обеспечения информационной безопасности	Характеристика информации, как объекта обеспечения безопасности Российской Федерации Гражданско-правовые механизмы обеспечения информационной безопасности Значение ноу-хау и режима коммерческой тайны в практической деятельности обеспечения информационной безопасности Система уголовно-правового обеспечения информационной безопасности Правовое регулирование некоторых сфер информатизации в России и за рубежом Защита приватности и персональных данных в законодательстве России и США. Электронный документ в России и США.
Тема 4. Информационно-аналитическое обеспечение системной безопасности объекта.	Описание субъекта информационной безопасности и выявление среди них критических. Присвоение категорий значимости. Анализ угроз безопасности, возможных действий нарушителя. Определение перечня угроз безопасности объекта. Разработка организационных и технических мер для обеспечения безопасности объектов критической информационной инфраструктуры. Подготовка сведений о результатах присвоения объекту информационной инфраструктуры одной из категорий значимости. Разработка модели угроз защищаемого объекта Разработка модели вероятного нарушителя. Технические каналы утечки информации Анализ каналов утечки информации. Построение модели угроз с учетом каналов утечки. Знакомство с существующими платформами для распознавания и обработки данных? OLAP-системы, технологии оперативного и интеллектуального анализа данных.
Тема 5. Синтез информационно-аналитических СБ	Режимы восприятия информации; средства автоматизации информационно-аналитической работы. Классификация и фильтрация данных. Моделирование и принятие решений в информационно-аналитической системе безопасности объектов. Аналитические системы поддержки принятия решений

Тематический план												
Названия содержательных модулей и тем	**Количество часов**											
	Очная форма обучения						**Заочная форма обучения**					
	всего	в т.ч.					всего	в т.ч.				
		лекции	практические	лабораторные	самостоятельная работа	индивидуальная работа		лекции	практические	лабораторные	самостоятельная работа	индивидуальная работа
Тема 1. Сущность, структура и задачи аналитики СБ.	16	2		2	12							
Тема 2. Стандарты обеспечения информационной безопасности	23	4		4	15							
Тема 3. Правовые методы обеспечения информационной безопасности	23	4		4	15							
Итого по содержательному модулю 1	59	9	-	9	36							
Тема 4. Информационно-аналитическое обеспечение системной безопасности объекта.	23	4		4	15							
Тема 5. Синтез информационно-аналитических СБ	23	4		4	15							
Итого по содержательному модулю 2	46	9	-	9	36							
Всего по дисциплине	**108**	**18**	**-**	**18**	**72**							

5. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ПРОВЕДЕНИЯ ЛЕКЦИОННЫХ, ПРАКТИЧЕСКИХ И ЛАБОРАТОРНЫХ ЗАНЯТИЙ

Темы лекционных занятий

№ п/п	*Название темы*	*Количество часов*
1	Понятие и сущность аналитики системы безопасности. Структура и задачи аналитики систем безопасности.	2
2	Формирование концепций правового регулирования информационной безопасности за рубежом и в России.	2
3	Стратегия формирования правовых методов информационной безопасности Российской федерации	2
4	Гражданско-правовые механизмы обеспечения информационной безопасности.	2
5	Правовое регулирование некоторых сфер информатизации в России и за рубежом	2
6	Информационно-аналитическое обеспечение системной безопасности объекта.	2
7	Знакомство с существующими платформами для распознавания и обработки данных?	2
8	Синтез информационно-аналитических СБ	2
9	Аналитические системы поддержки принятия решений	2
	ВСЕГО	**18**

Темы практических занятий

(Не предусмотрены)

Темы лабораторных занятий

№	Название темы	Количество часов
1.	1. Стандарты обеспечения информационной безопасности	2
2.	2. Правовые методы обеспечения информационной безопасности	2
3	3. Знакомство с Аналитической Платформой “Deductor”	2
4	4. Распознавание образов данных (Сеть Хемминга)	2
	5. Кластерная обработка данных (карты Кохонена)	2
5.	6 Классификация данных	2
	7. Фильтрация данных	4
	Защита отчетов	2
	ВСЕГО:	18

6. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОРГАНИЗАЦИИ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

Организация самостоятельной работы студентов

Самостоятельная работа студентов по курсу «Информационно-аналитические системы безопасости объектов» предусматривает:

– систематическое ведение конспекта лекций и повседневную проработку лекционного материала;

– изучение дополнительной технической литературы и интернет-источников, в т.ч. рекомендуемых этой программой;

– добросовестную подготовку к лабораторным занятиям;

– самостоятельное решение задач лабораторных работ;

– изучение дополнительного инструментария;

– своевременное выполнение и качественное оформление отчётов по лабораторным работам.

При желании студент может подготовить реферат или доклад по одной из тем, предложенных преподавателем.

№ п/п		***Количество часов***
1	Подготовка к лабораторным занятиям	45
2	Подготовка к лекционным занятиям и изучение дополнительной технической литературы и интернет-источников, в т.ч. рекомендуемых этой программой	45
3	Подготовка реферата	18
	ВСЕГО	**108**

7. ИНДИВИДУАЛЬНЫЕ ЗАДАНИЯ

(Не предусмотрены)

8. КОНТРОЛЬНЫЕ ВОПРОСЫ К ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

1. Понятие и сущность аналитики СБ.
2. Структура и задачи аналитики СБ.
3. Информационно-аналитические технологии СБ, их задачи.
4. Основные критерии оценки защищенности АС.
5. Концепция защиты АС и средств вычислительной техники (СВТ) по руководящим документам ФСТЭК РФ.
6. Критерии и классы защищенности средств вычислительной техники и автоматизированных систем.
7. Защита от угрозы нарушения конфиденциальности на уровне содержания информации.
8. Методы структурирования информации.
9. Методы поэтапной структуризации задач и морфологические методы.
10. Методы обработки и анализа числовых данных.
11. Угрозы конфиденциальности, целостности, доступности информации; раскрытие параметров информационной системы.

12. Задачи и определения информационно-аналитического (ИА) обеспечения СБ.
13. Организационные формы субъектов ИА работы.
14. Системы, управляемые потоком событий.
15. Поиск, отбор и анализ данных.
16. Неструктурированные текстовые данные.
17. Структурированные текстовые данные.
18. Резервное копирование данных.
19. Режимы восприятия информации.
20. Средства автоматизации информационно-аналитической работы.
21. Создание информационно-аналитических СБ (ИА СБ).
22. Составные части ИА СБ.
23. Стадии и технология создания ИА СБ.
24. Задачи аутентификации, понятие протокола аутентификации.
25. Основные схемы протоколов аутентификации.
26. Основные принципы построения систем защиты от НСД.
27. Классификация уровней защиты от НСД.
28. Программно-аппаратный состав средств защиты от НСД.
29. Аппаратные устройства для разграничения доступа в сети.
30. Разграничение доступа к ресурсам.
31. Какие задачи решает концепция обеспечения безопасности объектов охраны?
32. Категорирование объектов охраны.
33. Что такое безопасность защищаемого производственного объекта?
34. Охарактеризуйте цели анализа уязвимости объекта.
35. Что такое объект повышенной опасности?
36. Охарактеризуйте структуру системы обеспечения комплексной безопасности объекта.
37. Каким образом составляется модель нарушителя и возможные пути его проникновения на охраняемый объект..
38. Классификация нарушителей и угроз информационной безопасности.
39. Классификация технических средств охраны, области их применения.
40. Назначение, виды и основные характеристики радиоволновых и радиолучевых средств обнаружения.
41. Передатчик, антенная система и приемник как блок формирования полезного сигнала.
42. Назначение, классификация и основные характеристики оптических средств обнаружения.
43. Активные оптические средства обнаружения. Принцип действия, особенности применения.
44. Пассивные инфракрасные средства обнаружения.
45. Основные понятия и определения. Основы теории возбуждения и распространения сейсмических волн
46. Помехи в сейсмических средствах обнаружения.
47. Виды магнитометрических средств обнаружения, принципы их действия.
48. Основные характеристики магнитометрических средств обнаружения.
49. Характерные помехи при применении магнитометрических средств обнаружения магнитометрических средств обнаружения и способы их компенсации.
50. Назначение, виды и способы комбинирования средств обнаружения.
51. Какие нежелательные излучения радиопередающих устройств систем связи и передачи информации Вы знаете?
52. Какие нежелательные излучения технических средств обработки информации Вы знаете?:
53. Перечислите нежелательные электромагнитные связи
54. Как происходит утечка информации по цепям заземления?
55. Как происходит утечка информации по цепям питания?
56. Опишите виброакустический и электроакустический канал утечки информации
57. Утечка информации в волоконно-оптических линиях связи Основные понятия теории безопасности.

58. Ценность информации.
59. Общий анализ угроз информационной безопасности.
60. Основные виды атак на автоматизированные системы (АС).
61. Понятие политики безопасности.
62. Понятие и сущность аналитики СБ.
63. Структура и задачи аналитики СБ.
64. Информационно-аналитические технологии СБ, их задачи.
65. Основные критерии оценки защищенности АС.
66. Концепция защиты АС и средств вычислительной техники (СВТ) по руководящим документам ФСТЭК РФ.
67. Критерии и классы защищенности средств вычислительной техники и автоматизированных систем.
68. Защита от угрозы нарушения конфиденциальности на уровне содержания информации.
69. Методы структурирования информации.
70. Методы поэтапной структуризации задач и морфологические методы.
71. Методы обработки и анализа числовых данных.
72. Угрозы конфиденциальности, целостности, доступности информации; раскрытие параметров информационной системы.
73. Задачи и определения информационно-аналитического (ИА) обеспечения СБ.
74. Организационные формы субъектов ИА работы.
75. Системы, управляемые потоком событий.
76. Поиск, отбор и анализ данных.
77. Неструктурированные текстовые данные.
78. Структурированные текстовые данные.
79. Резервное копирование данных.
80. Режимы восприятия информации.
81. Средства автоматизации информационно-аналитической работы.
82. Создание информационно-аналитических СБ (ИА СБ).
83. Составные части ИА СБ.
84. Стадии и технология создания ИА СБ.
85. Задачи аутентификации, понятие протокола аутентификации.
86. Основные схемы протоколов аутентификации.
87. Основные принципы построения систем защиты от НСД.
88. Классификация уровней защиты от НСД.
89. Программно-аппаратный состав средств защиты от НСД.

9. ОБРАЗЕЦ МОДУЛЬНОГО КОНТРОЛЯ

ГОУ ВПО «ДОНЕЦКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ»
ФИЗИКО-ТЕХНИЧЕСКИЙ ФАКУЛЬТЕТ

Кафедра радиофизики и инфокоммуникационных технологий
Программа подготовки: академическая магистратура
Дисциплина «Информационно-аналитические системы безопасости объектов»
Направление подготовки: 10.04.01 Информационная безопасность, семестр 2.

МОДУЛЬНАЯ КОНТРОЛЬНАЯ РАБОТА ВАРИАНТ №1

1. Формирование концепций правового регулирования информационной безопасности за рубежом и в России
2. Какой вид имеет активационная функция для сети Хемминга?
3. Задача.

Утверждено на заседании кафедры. Зав. кафедрой РФ и ИКТ _____ В.В. Данилов

№ ____ от _____201_г. Экзаменатор _____ О.Г. Шелехова

Критерии оценивания модульного контроля

Номер задания	***Количество баллов***
1	10
2	10
3	10
Всего	***30***

10. ОБРАЗЕЦ ЭКЗАМЕНАЦИОННОГО БИЛЕТА

Вопросы к экзамену

1. Аппаратные устройства для разграничения доступа в сети.
2. Разграничение доступа к ресурсам.
3. Роль и место анализа в процессе принятия решения.
4. Этапы аналитического исследования.
5. Классификация источников и методов сбора (получения) информации.
6. Методы анализа и прогнозирования как объект автоматизации.
7. Требования, предъявляемые к информационно-аналитическим системам.
8. Планирование разведывательной деятельности.
9. Модель конкурентной среды М. Портера.
10. Методика сбора информации о юридическом лице.
11. Методика сбора информации о физическом лице.
12. Система конкурентной разведки на предприятии.
13. Основные методы противодействия промышленному шпионажу.
14. Планирование и организация контрразведывательной деятельности.
15. Агенты влияния.
16. Классификация внутренних нарушителей (инсайдеров) и методы борьбы с ними.

17. Принципы работы систем анализа защищенности. Требования к системам.
18. Отечественный рынок информационно-аналитических систем.
19. Подходы к выполнению анализа средствами информационных технологий.
20. Составные части информационно-аналитических систем безопасности.
21. Управление информационно-аналитическими системами безопасности.
22. Интеллектуальный анализ данных
23. Что является исходными данными для проведения оценки и анализа угроз безопасности объектов?
24. Дать определение нарушителя, по каким критериям они классифицируются?
25. Дать определение технического канала утечки информации, назвать типы.
26. Дать определение носителя защищаемой информации, назвать типы.
27. Какие сведения включает пространственная модель каналов утечки?
28. Что такое формализованная и неформализованная модель нарушителя?
29. Перечислите цели и задачи вероятного нарушителя.
30. Какое оборудование относят к виброакустические каналам утечки информации?
31. Дать описание четырех категорий нарушителя.
32. Что представляет собой матрица угроз/средств защит и матрица вероятностей наступления угроз?
33. Какие задачи решает концепция обеспечения безопасности объектов охраны?
34. Категорирование объектов охраны.
35. Что такое безопасность защищаемого производственного объекта?
36. Охарактеризуйте цели анализа уязвимости объекта.
37. Что такое объект повышенной опасности?
38. Охарактеризуйте структуру системы обеспечения комплексной безопасности объекта.
39. Каким образом составляется модель нарушителя и возможные пути его проникновения на охраняемый объект..
40. Классификация нарушителей и угроз информационной безопасности.
41. Классификация технических средств охраны, области их применения.
42. Назначение, виды и основные характеристики радиоволновых и радиолучевых средств обнаружения.
43. Передатчик, антенная система и приемник как блок формирования полезного сигнала.
44. Назначение, классификация и основные характеристики оптических средств обнаружения.
45. Активные оптические средства обнаружения. Принцип действия, особенности применения.
46. Пассивные инфракрасные средства обнаружения.
47. Основные понятия и определения. Основы теории возбуждения и распространения сейсмических волн
48. Помехи в сейсмических средствах обнаружения.
49. Виды магнитометрических средств обнаружения, принципы их действия.
50. Основные характеристики магнитометрических средств обнаружения.
51. Характерные помехи при применении магнитометрических средств обнаружения магнитометрических средств обнаружения и способы их компенсации.
52. Назначение, виды и способы комбинирования средств обнаружения.
53. Какие нежелательные излучения радиопередающих устройств систем связи и передачи информации Вы знаете?
54. Какие нежелательные излучения технических средств обработки информации Вы знаете?:
55. Перечислите нежелательные электромагнитные связи
56. Как происходит утечка информации по цепям заземления?
57. Как происходит утечка информации по цепям питания?
58. Опишите виброакустический и электроакустический канал утечки информации
59. Утечка информации в волоконно-оптических линиях связи
60. Знакомство с Аналитической Платформой “Deductor”
61. Какие существуют другие платформы для распознавания и обработки данных?

62. Какие возможности имеет АП Deductor для распознавания данных?
63. Какие возможности имеет АП Deductor для обработки данных?
64. Какие параметры доступны для мастера экспорта данных?
65. В чем заключается процедура визуализации данных?
66. Что такое «Редактор метаданных» в DeductorStudio?
67. Как создать новое пустое хранилище данных?
68. Как сделать иерархию измерений?
69. Какие типы данных могут быть у объектов хранилища?
70. Чем факт отличается от измерения?
71. Какой алгоритм генерации ассоциативных правил имеется в Deductor?
72. Какие входные поля набора данных необходимы для запуска обработчика Ассоциативные правила в Deductor?
73. Какие специализированные визуализаторы предлагаются к узлу- обработчику Ассоциативные правила?
74. Распознавание образов данных (Сеть Хемминга)
75. Приведите примеры использования сети Хемминга.
76. Сколько слоев имеет сеть Хемминга?
77. Какую роль играют обратные связи?
78. Каким образом определяется распознаваемый образ?
79. Какой вид имеет активационная функция для сети Хемминга?
80. Совпадает ли количество входов и выходов в сети Хемминга?
81. Кластерная обработка данных (карты Кохонена)
82. Для чего используются карты Кохонена?
83. По какому принципу происходит перенос многомерного пространства на пространство меньшей размерности?
84. Какие метрики используются при разбиении на кластеры
85. Целесообразность применения карт Кохонена при кластеризации данных.
86. Классификация данных
87. В чем суть классификации данных?
88. Отличие классификации от кластеризации.
89. Какие существуют методы классификации кроме нейросетевого?
90. Целесообразность применения нейросетевого метода для классификации данных.
91. Как определяется погрешность классификации?
92. Фильтрация данных
93. В чем заключается суть работы фильтра Калмана?
94. Пояснить, что происходит с фильтром, если дисперсия $\omega(k)$ больше дисперсии $v(k+1)$ и почему?
95. В чем смысл уравнение состояния?
96. Что представляет уравнение измерения?
97. Поясните возможность применения фильтра Калмана для нестанционарных процессов.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ ДНР
ДОНЕЦКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ
Физико-технический факультет, кафедра радиофизики
Дисциплина **«Информационно-аналитические системы безопасности объектов»**
специальность 10.03.01, семестр 3.

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1. Сравнительный анализ правового обеспечения информационной безопасности в России и за рубежом
2. Целесообразность применения карт Кохонена при кластеризации данных
3. Задача.

Утверждено на заседании кафедры. Зав. кафедрой _____ Данилов В.В.

№ ____ от _____20 г. Экзаменатор _____ Шелехова О.Г..

11. ОБРАЗЕЦ ТЕСТОВОГО ЗАДАНИЯ

(Не предусмотрено)

12. КРИТЕРИИ ОЦЕНИВАНИЯ

Согласно модульному принципу организации учебного процесса содержание учебного курса состоит из лабораторных работ, двух модульных контролей и экзамена. Каждый модуль состоит из лабораторных работ.

При защите лабораторной работы выставляются: за получение допуска к выполнению работы – максимум 1 балл; за выполнения работы, оформление отчета – максимум 1 балл; за умение объяснить результаты работы, объяснить проведенные вычисления, знание основных законов, которые рассматриваются в работе, – максимум 1 балл.

Еще 1 балл студент может получить за ответ на контрольный вопрос, который нуждается в фундаментальной подготовке, оценка выставляется с точностью до 0,5 баллов в зависимости от качества ответа.

Студент должен выполнить лабораторную работу по графику и защитить ее не позднее следующего занятия, за каждое просроченное занятие отнимается 0,5 балла от набранной суммы баллов, за досрочное выполнение и защиту работы добавляется 0,5 балла. В каждом из модулей студент должен выполнить 4 лабораторных работы, за каждую из которых может получить до 5 баллов.

Еще один балл в каждом модуле студент может получить за добросовестное, систематическое ведение конспекта.

Экзаменационный билет содержит две задачи и теоретический вопрос. Ответ на теоретический вопрос оценивается в зависимости от полноты от 0 до 10 баллов, ответы на задачи - от 0 до 20 баллов. Максимальная сумма балов за экзамен составляет 40 баллов.

Оценка знаний студентов проводится по 100-балльной шкале согласно следующим критериям:

По учебной дисциплине предполагается проведение модульного контроля, выполнение индивидуальной работы и проведение экзамена.

Распределение баллов, которые могут получить студенты в процессе изучения дисциплины

Организационно-учебная работа студента	**СРС**			**Всего**
	Экзаменационная работа	**Модульный контроль**	**Лабораторные работы**	
Max **13** баллов	max 30 баллов	max 25 баллов	max 32 баллов	**100** баллов
Экспресс-опрос на лекциях и активность на лабораторных занятиях; проверка конспектов	Выполнение экзаменационной работы	Выполнение модульной контрольной работы	Подготовка отчетов по лабораторным работам	

Шкала соответствия баллов национальной шкале

Оценка по шкале ECTS	**Оценка по 100-балльной шкале**	**Оценка по государственной шкале (экзамен, дифференцированный зачет)**	**Оценка по государственной шкале (зачет)**
A	90-100	5 (отлично)	зачтено
B	80-89	4 (хорошо)	зачтено
C	75-79	4 (хорошо)	зачтено
D	70-74	3 (удовлетворительно)	зачтено
E	60-69	3 (удовлетворительно)	зачтено
FX	35-59	2 (неудовлетворительно) с возможностью повторной сдачи	не зачтено
F	0-34	2 (неудовлетворительно) с возможностью повторной сдачи при условии обязательного набора дополнительных баллов	не зачтено

13. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОГО ПРОЦЕССА

Лекционные занятия проводятся в аудитории, оснащенной мультимедийной техникой и доской.

Лабораторные занятия проводятся в лаборатории, оборудованной столами, доской.

Научная библиотека ГОУ ВПО «ДонНУ» располагает обширным фондом учебной и научной литературы по курсу.

14. РЕКОМЕНДОВАННАЯ ЛИТЕРАТУРА

№ п/п	**Наименование**	**Кол-во экземпляров в библиотеке ДонНУ**	**Наличие электронной версии в ЭБС**
	Основная литература		
1.	Информационно-аналитические системы безопасности объектов [Текст] : учебное пособие для магистров высших учебных заведений, обучающихся по направлению подготовки 10.04.01 Информационная безопасность / [Шелехова О.Г.] ; ДОННУ. – Донецк : Цифровая типография, 2019. – 125 с.		+

№ п/п	Наименование	Кол-во экземпляров в библиотеке ДонНУ	Наличие электронной версии в ЭБС
2.	Лабораторный практикум по информационно-аналитическим системам безопасности объектов: учебно-методическое пособие [Текст] : учебно-методическое пособие для магистров высших учебных заведений, обучающихся по направлению подготовки 10.04.01 Информационная безопасность / [Шелехова О.Г.] ; ДОННУ. – Донецк : Цифровая типография, 2019. – 83 с.		+
Дополнительная литература			
1.	Минаев, Г. А. Безопасность организации : учебник / Г. А. Минаев ; Ин-т управления и безопасности. - Київ : КНТ, 2009. - 440 с.	3	-
2.	Корт, С. С. Теоретические основы защиты информации : Учеб. пособие для студентов вузов, обучающихся по группе спец. в обл. информ. безопасности / С. С. Корт. - М. : Гелиос АРВ, 2004. - 233 с	0	+

15. Информационные ресурсы

1. Белорусский журнал «Технологии безопасности» // http: //www.journals.proektant.by/index.php?journal=tehnologii_bezopasnosti
2. Техническое обеспечение безопасности объектов «Алгоритм безопасности» // http: // https://algoritm.org/arch/arch.php?id=67&a=1491
3. Журнал «Техническая защита» // http://www.tzmagazine.ru
4. Государственная публичная научно-техническая библиотека // www.gpntb.ru.
5. Российская национальная библиотека // www.nns.ru.
6. Национальная электронная библиотека // www.nlr.ru.
7. Учебный центр компьютерных технологий «Микроинформ» // www.microinform.ru.
8. Центр компьютерного обучения МГТУ им. Н.Э.Баумана // www.tests.specialist.ru.
9. Журнал «Открытые системы» // www.osp.ru.

16. ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

1. Windows 7 PRO (корпоративная лицензия ДОННУ № 46484614);
2. Microsoft Office (корпоративная лицензия ДОННУ лицензия № 46472919);
3. Microsoft Visual Studio (лицензия программы DreamSpark для высших учебных заведений);

ИСПОЛЬЗОВАНИЕ ЭЛЕКТРОННОГО ОБУЧЕНИЯ И ДИСТАНЦИОННЫХ ОБРАЗОВАТЕЛЬНЫХ ТЕХНОЛОГИЙ

При реализации программы дисциплины могут использоваться следующие виды электронного взаимодействия преподаватель-студент:

- размещение учебных материалов в облачных хранилищах преподавателей для использования студентами при подготовке к занятиям;
- рассылка по электронной почте материалов и заданий для выполнения, проверка выполненных заданий;
- поддержка странички преподавателя и групп преподаватель-студенты в социальных сетях для обеспечения текущего контроля работы студентов

Рабочая программа рассмотрена и переутверждена на заседании _____ с изменениями (без изменений) на 20____ год.

Протокол № ___ от «_____» _____ 20____ г.

Заведующий кафедрой _____