Негосударственное аккредитованное некоммерческое частное образовательное учреждение высшего образования
«Академия маркетинга и социально-информационных технологий – ИМСИТ»
(г. Краснодар)

(НАН ЧОУ ВО Академия ИМСИТ)

УТВЕРЖДАЮ
Проректор по учебной работе, доцент

_____Н.И. Севрюгина

20.11.2023

Б1.В.08
Комплексная защита объектов информатизации
рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Кафедра математики и вычислительной техники**

Учебный план 10.03.01 Информационная безопасность

Квалификация **бакалавр**
Форма обучения **очная**
Общая трудоемкость **5 ЗЕТ**

Часов по учебному плану 180
в том числе:
аудиторные занятия 96
самостоятельная работа 48
контактная работа во время промежуточной аттестации (ИКР) 0
часов на контроль 34,7

Виды контроля в семестрах:
экзамены 8

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**8 (4.2)**		Итого	
Недель	7 4/6			
Вид занятий	УП	РП	УП	РП
Лекции	32	32	32	32
Лабораторные	64	64	64	64
Контактная работа на аттестации (в период экз. сессий)	0,3	0,3	0,3	0,3
Консультации перед экзаменом	1	1	1	1
В том числе в форме практ.подготовки	10	10	10	10
Итого ауд.	96	96	96	96
Контактная работа	97,3	97,3	97,3	97,3
Сам. работа	48	48	48	48
Часы на контроль	34,7	34,7	34,7	34,7
Итого	180	180	180	180

Программу составил(и):
к.т.н., доцент, Капустин С.А.

Рецензент(ы):
д.т.н., Профессор кафедры информатики и вычислительной техники КубГТУ,, Хисамов Ф.Г.

Рабочая программа дисциплины
Комплексная защита объектов информатизации

разработана в соответствии с ФГОС ВО:
Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 10.03.01 Информационная безопасность (приказ Минобрнауки России от 17.11.2020 г. № 1427)

составлена на основании учебного плана:
10.03.01 Информационная безопасность
утвержденного учёным советом вуза от 20.11.2023 протокол № 3.

Рабочая программа одобрена на заседании кафедры
Кафедра математики и вычислительной техники

Протокол от 13.10.2023 г. № 3

Зав. кафедрой Исикова Наталья Павловна

Согласовано с представителями работодателей на заседании НМС, протокол № 3 от 20.11.2023.

Председатель НМС проф. Павелко Н.Н.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Формирование у студентов знаний в области комплексной защиты объектов
1.2	информатизации, построения систем информационной безопасности с
1.3	использованием технических средств охраны, освоение дисциплинарных
1.4	компетенций, связанных с раскрытием базовых и расширенных технологий
1.5	обеспечения информационной безопасности сложных технических объектов и
1.6	систем.

Задачи: изучение основных положений, понятий и категорий, относящихся к базовым и расширенным технологиям обеспечения информационной безопасности;
изучение принципов организации, комплексного подхода к выбору средств и технологий обеспечения информационной безопасности объектов защиты
изучение методов проектирования систем безопасности охраняемого объекта;
изучение принципов работы технических средств охраны;
определение критериев защищенности охраняемого объекта;
освоение механизмов защиты охраняемых объектов;
формирование правильного подхода к проблемам информационной безопасности, который начинается с выявления субъектов информационных отношений и интересов этих субъектов, связанных с использованием информационных систем (ИС)

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.В
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Структуры и алгоритмы обработки данных
2.1.2	Методы защиты программного обеспечения
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Выполнение и защита выпускной квалификационной работы

3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ, ИНДИКАТОРЫ ИХ ДОСТИЖЕНИЯ и планируемые результаты обучения

ПК-5: Способен выполнять работы по обеспечению информационной безопасности автоматизированных систем на всех этапах их жизненного цикла

ПК-5.1: Проверяет соответствие внедряемых решений и средств для обеспечения информационной безопасности требованиям реализуемой политики безопасности

Знать

Уровень 1	Минимальный необходимый уровень знаний для проверки соответствия внедряемых решений и средств для обеспечения информационной безопасности требованиям реализуемой политики безопасности
Уровень 2	Уровень знаний для проверки соответствия внедряемых решений и средств для обеспечения информационной безопасности требованиям реализуемой политики безопасности в объёме, соответствующем программе подготовки, допущено несколько негрубых ошибок
Уровень 3	Уровень знаний для проверки соответствия внедряемых решений и средств для обеспечения информационной безопасности требованиям реализуемой политики безопасности в объёме, соответствующем программе подготовки, без ошибок

ПК-5.2: Восстанавливает работоспособность автоматизированных систем после инцидентов информационной безопасности

Уметь

Уровень 1	Продемонстрированы основные умения восстанавливать работоспособность автоматизированных систем после инцидентов информационной безопасности , решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме
Уровень 2	Продемонстрированы основные умения восстанавливать работоспособность автоматизированных систем после инцидентов информационной безопасности, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объёме, но некоторые с недочётами
Уровень 3	Продемонстрированы основные умения восстанавливать работоспособность автоматизированных систем после инцидентов информационной безопасности, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объёме

ПК-5.3: Проводит операции вывода защищённых автоматизированных систем из эксплуатации

Владеть

Уровень 1	Имеется минимальный набор навыков проведения операции вывода защищённых автоматизированных систем из эксплуатации с негрубыми ошибками и некоторыми недочётами
Уровень 2	Продемонстрированы базовые навыки проведения операции вывода защищённых автоматизированных систем из эксплуатации с некоторыми недочётами
Уровень 3	Продемонстрированы базовые навыки проведения операции вывода защищённых автоматизированных систем из эксплуатации без ошибок и недочётов

ПК-7: Способен определять уровень защищённости автоматизированных систем	
ПК-7.1: Формулирует целевые показатели функционирования защищенных автоматизированных систем	
Знать	
Уровень 1	Минимальный необходимый уровень знаний целевых показателей функционирования защищенных автоматизированных систем
Уровень 2	Уровень знаний целевых показателей функционирования защищенных автоматизированных систем в объёме, соответствующем программе подготовки, допущено несколько негрубых ошибок
Уровень 3	Уровень знаний целевых показателей функционирования защищенных автоматизированных систем в объёме, соответствующем программе подготовки, без ошибок
ПК-7.2: Анализирует уязвимости автоматизированных систем в соответствии с нормативными документами	
Уметь	
Уровень 1	Продемонстрированы основные умения анализировать уязвимости автоматизированных систем в соответствии с нормативными документами, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература и эл. ресурсы	Практ. подг.
	Раздел 1. Раздел 1					
1.1	Понятия и определения технических средств охраны. Структура автоматизированной системы охраны /Лек/	8	6	ПК-5.1 ПК-5.2 ПК-5.3 ПК-7.1 ПК-7.2 ПК-7.3 ПК-8.1 ПК-8.2 ПК-8.3 ПК-8.4 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3	
1.2	Понятия и определения технических средств охраны. Структура автоматизированной системы охраны /Лаб/	8	12	ПК-5.1 ПК-5.2 ПК-7.2 ПК-7.3 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3	2
1.3	Понятия и определения технических средств охраны. Структура автоматизированной системы охраны /Ср/	8	8	ПК-5.1 ПК-5.2 ПК-7.2 ПК-7.3 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3	
1.4	Варианты программно-аппаратной реализации ТСО /Лек/	8	6	ПК-5.1 ПК-5.2 ПК-7.2 ПК-7.3 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3	
1.5	Варианты программно-аппаратной реализации ТСО /Лаб/	8	12	ПК-5.1 ПК-5.2 ПК-7.2 ПК-7.3 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3	2
1.6	Варианты программно-аппаратной реализации ТСО /Ср/	8	8	ПК-5.1 ПК-5.2 ПК-7.2 ПК-7.3 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3	

1.7	Методология разработки концепции комплексного обеспечения безопасности объектов охраны /Лек/	8	4	ПК-5.1 ПК-5.2 ПК-7.2 ПК-7.3 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3	
1.8	Методология разработки концепции комплексного обеспечения безопасности объектов охраны /Лаб/	8	10	ПК-5.1 ПК-5.2 ПК-7.2 ПК-7.3 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3	2
1.9	Методология разработки концепции комплексного обеспечения безопасности объектов охраны /Ср/	8	8	ПК-5.1 ПК-5.2 ПК-7.2 ПК-7.3 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3	
1.10	Общий подход к категорированию объектов охраны /Лек/	8	6	ПК-5.1 ПК-5.2 ПК-7.2 ПК-7.3 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3	
1.11	Общий подход к категорированию объектов охраны /Лаб/	8	10	ПК-5.1 ПК-5.2 ПК-7.2 ПК-7.3 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3	2
1.12	Общий подход к категорированию объектов охраны /Ср/	8	8	ПК-5.1 ПК-5.2 ПК-7.2 ПК-7.3 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3	
1.13	Классификация нарушителей информационной безопасности, угроз ИБ /Лек/	8	6	ПК-5.1 ПК-5.2 ПК-7.2 ПК-7.3 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3	
1.14	Классификация нарушителей информационной безопасности, угроз ИБ /Лаб/	8	10	ПК-5.1 ПК-5.2 ПК-7.2 ПК-7.3 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3	1
1.15	Классификация нарушителей информационной безопасности, угроз ИБ /Ср/	8	8	ПК-5.1 ПК-5.2 ПК-7.2 ПК-7.3 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3	
1.16	Классификация технических средств охраны, необходимых для построения комплексной системы защиты информации /Лек/	8	4	ПК-5.1 ПК-5.2 ПК-7.2 ПК-7.3 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3	
1.17	Классификация технических средств охраны, необходимых для построения комплексной системы защиты информации /Лаб/	8	10	ПК-5.1 ПК-5.2 ПК-7.2 ПК-7.3 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3	1
1.18	Классификация технических средств охраны, необходимых для построения комплексной системы защиты информации /Ср/	8	8	ПК-5.1 ПК-5.2 ПК-7.2 ПК-7.3 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3	
	Раздел 2. Промежуточная аттестация					

2.1	Консультация /Консл/	8	1	ПК-5.1 ПК-5.2 ПК-7.2 ПК-7.3 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3	
2.2	Экзамен /КАЭ/	8	0,3	ПК-5.1 ПК-5.2 ПК-7.2 ПК-7.3 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3	

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

5.1. Контрольные вопросы и задания

1. Методологические основы организации КСЗИ.
2. Методика определения состава защищаемой информации.
3. Значение носителей защищаемой информации как объектов защиты.
4. Определение источников дестабилизирующего воздействия на информацию и видов их воздействия в автоматизированных системах.
5. Факторы, влияющие на выбор компонентов КСЗИ в распределенных информационных системах.
6. Методы и средства защиты информации в АС от промышленного шпионажа и диверсий.
7. Основные этапы разработки КСЗИ в АС.
8. Компьютерные вирусы и механизмы борьбы с ними.
9. Защита информации в распределенных АС.
10. Понятие и виды контроля функционирования КСЗИ в распределенных информационных системах.

По согласованию с преподавателем тема доклада может быть выбрана студентом самостоятельно.

5.2. Темы письменных работ

1.Случайные и преднамеренные угрозы информации в компьютерных системах
2. Защита информации в АС от случайных угроз.
3. Методы и средства защиты информации в АС от промышленного шпионажа и диверсий.
4. Методы и средства защиты от электромагнитных излучений и наводок.
5. Методы защиты от несанкционированного изменения структур АС.
6. Защита от внедрения аппаратных закладок на этапе разработки и производства.
7. Защита информации в АС от несанкционированного доступа.
8.Криптографические методы защиты информации.
9. Компьютерные вирусы и механизмы борьбы с ними. Защита информации в распределенных АС.
10. Понятие и назначение КСЗИ. Концепция создания защищенных АС. Требования, предъявляемые к КСЗИ
11. Факторы, влияющие на организацию КСЗИ
12. Основные этапы разработки КСЗИ
13. Определение компонентов КСЗИ
14. Функциональная модель КСЗИ
15. Организационная модель КСЗИ
16. Информационная модель КСЗИ
17. Классификация информации по видам тайн и степени конфиденциальности
18. Методика определения состава защищаемой информации
19. Порядок разработки и внедрения перечней сведений конфиденциального характера на предприятии. Порядок внесения изменений и дополнений в перечень.
20. Характеристика основных стадий создания КСЗИ.
21. Назначение и структура задания на проектирование, технического задания, техникоэкономического обоснования.
22. Моделирование комплексной защиты автоматизированных систем.
23. Математическая постановка задачи разработки комплексной системы защиты информации.
24. Подходы к оценке эффективности КСЗИ.
25. Выбор показателей эффективности и критериев оптимальности КСЗИ.
26. Общая характеристика подходов к оценке эффективности систем защиты информации
27. Вероятностный подход к оценке эффективности системы защиты информации
28. Статистические и экспертные методы оценки эффективности системы защиты информации
29. Показатели защищенности системы защиты информации
30. Содержательная характеристика этапов разработки КСЗИ

31. Управление КСЗИ в условиях чрезвычайных ситуаций
32. Понятие и виды контроля функционирования КСЗИ.
33. Цель проведения контрольных мероприятий и методы контроля. Анализ и использование результатов проведения контрольных мероприятий.
34. Значение материально-технического обеспечения функционирования КСЗИ.
35. Значение нормативно-методического обеспечения функционирования КСЗИ.
36. Состав нормативно-методических документов по обеспечению функционирования КСЗИ, их назначение, структура и содержание.
37. Определение состава кадрового обеспечения функционирования КСЗИ.
38. Распределение функций по защите информации между руководством предприятия, службой защиты информации, специальными комиссиями и пользователями защищаемой информации, обеспечение взаимодействия между ними.
39. Разработка нормативных документов, регламентирующих деятельность персонала по защите информации в АС. Подбор и обучение персонала .

5.3. Фонд оценочных средств

Задание в закрытой форме:
Количественный состав службы безопасности зависит, прежде всего от
a. Типа циркулирующей в ней конфиденциальной информации
b. От возможностей фирмы
c. Нормативных документов регуляторов
d. Численности штата
Задание в открытой форме:
… критерии предъявляются к действиям разработчика системы, документам для оценивания и работе самой организации. Включают требования доверия к мерам к СЗИ в информационных системах, а также к их разработке и эксплуатации.
Задание на установление правильной последовательности,
Надиктовать тестовую информацию (с обязательным указанием номера точки, в которой производиться измерение, и расстояния до нее от центра антенны ЛГШ-104), расположить антенну ЛГШ-104 на столе; повторить измерения во всех 7 контрольных точках; Включить ЛГШ-104 и провести измерение среднего значения напряженности поля Е; включить диктофоны на запись; переместить диктофоны на 15 см в заданную сторону от центра антенныЛГШ-104; поместить антенну прибора ЛГШ-104 на подставку, находящуюся под столом; повторить измерения.

Задание на установление соответствия:
1 Случайный нарушитель
2 Неподготовленный нарушитель
3 Подготовленный нарушитель
4 Осведомленный нарушитель
5 Сотрудник предприятия или охранник
А обладающий специальной подготовкой, имеющий сведения об организации системы охраны на объекте
Б обладающий специальной подготовкой, часто действующий в сговоре с осведомленным нарушителем (характерно для крупного предприятия).
Г проникающий на объект со специальной целью и предполагающий возможность охраны объекта, но не имеющий представления о системе охраны и принципах ее функционирования.
Д имеющий информацию о возможных методах обхода действующих средств охраны, прошедший соответствующую подготовку скрытно преодолевать зоны обнаружения средств из состава комплексной системы безопасности.
Е не знающий, что объект охраняется и не имеющий специальной цели проникновения на объект.
Компетентностно-ориентированная задача:
Рассчитать требуемое кол-во ГШ-1000 для зашумления помещения с ПК если его размеры следующие длина 20 м ширина 6 м.

5.4. Перечень видов оценочных средств

Задания со свободно конструируемым ответом (СКО) предполагает составление развернутого ответа на теоретический вопрос. Задание с выбором варианта ответа (ОВ, в задании данного типа предлагается несколько вариантов ответа, среди которых верный(ые). Задания со свободно конструируемым ответом (СКО) предполагает составление развернутого ответа, включающего полное решение задачи с пояснениями.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год
Л1.1	Дергачев К. В., Титарев Д. В.	Защита информации: лабораторный практикум: Учебное пособие	Москва: Русайнс, 2021, URL: https://book.ru/book/940250
Л1.2	Москвитин Г. И.	Комплексная защита информации в организации: Монография	Москва: Русайнс, 2020, URL: https://book.ru/book/934814

	Авторы, составители	Заглавие	Издательство, год
Л1.3	Баранова Е.К., Бабаш А.В.	Информационная безопасность и защита информации: Учебное пособие	Москва: Издательский Центр РИО□, 2021, URL: http://znanium.com/catalog/document?id=364911

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год
Л2.1	Шаньгин В.Ф.	Комплексная защита информации в корпоративных системах: Учебное пособие	Москва: Издательский Дом "ФОРУМ", 2020, URL: http://znanium.com/catalog/document?id=358722
Л2.2	Сычев Ю.Н.	Защита информации и информационная безопасность: Учебное пособие	Москва: ООО "Научно-издательский центр ИНФРА-М", 2022, URL: http://znanium.com/catalog/document?id=388766
Л2.3	Хорев П. Б.	Программно-аппаратная защита информации: Учебное пособие	Москва: ООО "Научно-издательский центр ИНФРА-М", 2022, URL: https://znanium.com/catalog/document?id=397282

6.3.1. Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства

6.3.1.1	Windows 10 Pro RUS Операцинная система – Windows 10 Pro RUS Подписка Microsoft Imagine Premium – Order №143659 от 12.07.2021
6.3.1.2	7-Zip Архиватор 7-Zip Программное обеспечение по лицензии GNU GPL
6.3.1.3	Яндекс Браузер Браузер Яндекс Браузер Лицензионное соглашение на использование программ Яндекс Браузер https://yandex.ru/legal/browser_agreement/
6.3.1.4	Mozilla Firefox Браузер Mozilla Firefox Программное обеспечение по лицензии GNU GPL
6.3.1.5	LibreOffice Офисный пакет LibreOffice Программное обеспечение по лицензии GNU GPL

6.3.2. Перечень профессиональных баз данных и информационных справочных систем

6.3.2.1	Консультант Плюс http://www.consultant.ru

7. МТО (оборудование и технические средства обучения)

Ауд	Наименование	ПО	Оснащение
114а	Лаборатория программно-аппаратных средств защиты информации	Windows 10 Pro RUS 7-Zip Яндекс Браузер Mozilla Firefox LibreOffice LibreCAD Inkscape Notepad++. 1С:Предприятие 8. Комплект Kaspersky Endpoint Security MS Access 2016 MS Project Pro 2016 MS SQL Server 2019 MS SQL Server Management Studio 18.8 MS Visio Pro 2016 MS Visual Studio Community Edition Visual Studio Code Blender Gimp Maxima Oracle VM VirtualBox PostgreSQL IntelliJ IDEA PyCharm Community Edition Eclips Adobe Reader DC NetBeans IDE ZEAL Klite Mega Codec Pack MS Office Standart 2010	Стол - 20 шт., стул - 22 шт., рабочее место преподавателя – 1 шт., персональный компьютер с выходом в интернет - 21 шт., доска учебная – 1 шт., многофункциональное устройство – 1 шт., мультимедийный проектор – 1 шт., проекционный экран – 1 шт., интерактивная доска WR-84A10 с проектором ViewSonic PS501X - 1 шт., соответствующее программное обеспечение Коммутатор LincSys SR224G – 1 шт., проектор ViewSonic PJD5232 – 1 шт., проекционный экран Luma – 1 шт., шкаф телекоммуникационный – 1 шт., ИБП SMART UPS 2000 – 1 шт., коммутатор Cisco Catalist 2960 – 3 шт., концентратор AlterPath 16 port – 1 шт., маршрутизатор Cisco-2800 – 4 шт., маршрутизатор Cisco-2811 – 2 шт., модуль 2-port – 6 шт., панель коммутационная 2 шт., Шнур V.35 Cable – 12 шт., витая пара, коннектор RJ-45, инструмент для зачистки кабеля UTP – 2 шт., протяжка кабельная, d=3,5 мм 10 м – 1 шт., тестер МЕГЕОН 40060/Шт. – 1 шт., инструмент для обжима витой пары – 5 шт., Тестер кабельный – 5 шт., инструмент для заделки кабеля витая пара тип Krone с крючками – 3 шт., Р телефон GrandStream GXP1610 – 2 шт., комплект для монтажа СКС (патч-панель 1U kat.5e UTP 24 порта-1 шт., инструмент обжимной для RJ-45 1 шт., инструмент для зачистки кабеля 1 шт., инструмент для разделки контактов - 1 шт., LAN тестер 1 шт.) – 2 шт., роутер Wi-Fi роутер Keenetic – 2 шт., сервер GA-870A-USB3/AMD-Phenom(tm)-II-X4-945/ DDR3-1333-4Гб/SSD Flexis 120Gb/WD5000AAKX/Radeon HD-5800/Realtek PCIe GBE – 1 шт., аппаратные средства аутентификации пользователя: Соболь – 3 шт., эмуляторы активного сетевого оборудования в составе: Cisco Packet Tracer, Minine, Line Network Emulator, Marionnet – 21 шт., стенды для исследования параметров сетевого трафика в составе:

		Traffic inspector Special Unlimited Ramus Educational Micro-Cap Evaluation vGate Secren Net Studio Secren Net LSP Astra Linux Special Edition	WireShark, Snort, Colasoft Capsa Free, Ostinato, Suricata, Hping – 21 шт., средства антивирусной защиты: Kaspersky Endpoint Security для бизнеса, Dr.Web Security Space, средства защиты информации: ОС Astra Linux SE 1.7 «Смоленск» – 21 шт., Secret Net Studio – 21 шт., Secret Net LSP – 21 шт., vGate – 21 шт., стенд «Континент» – 21 шт., средства криптографической защиты информации: PGP – 21 шт., КриптоПро УЦ, – 21 шт., КриптоАРМ – 21 шт., КриптоПро CSP – 21 шт., межсетевые экраны: встроенные в ОС, стенд «Континент» – 21 шт., IPTables – 21 шт., Colasoft Capsa Free – 21 шт., средства обнаружения компьютерных атак: XSpider – 21 шт., MaxPatrol VM – 21 шт.
123	Кабинет информационной безопасности	Windows 10 Pro RUS 7-Zip Яндекс Браузер Mozilla Firefox LibreOffice LibreCAD Inkscape Notepad++. 1С:Предприятие 8. Комплект Kaspersky Endpoint Security MS Access 2016 MS Project Pro 2016 MS SQL Server 2019 MS SQL Server Management Studio 18.8 MS Visio Pro 2016 MS Visual Studio Community Edition Visual Studio Code Blender Gimp Maxima Oracle VM VirtualBox StarUML V1 PostgreSQL IntelliJ IDEA PyCharm Community Edition Eclips Adobe Reader DC Arduino Software (IDE) NetBeans IDE ZEAL ARIS Express Archimate Ramus Educational Micro-Cap Evaluation gvSIG Desktop Python	Стол - 20 шт., стул - 21 шт., рабочее место преподавателя – 1 шт., персональный компьютер с выходом в интернет - 21 шт., доска учебная – 1 шт., многофункциональное устройство – 1 шт., мультимедийный проектор – 1 шт., проекционный экран – 1 шт., соответствующее программное обеспечение
Читальный зал	Информационно-библиотечный центр (помещение для самостоятельной работы обучающихся)	7-Zip Яндекс Браузер Mozilla Firefox LibreOffice LibreCAD Inkscape Notepad++. Kaspersky Endpoint Security MS Access 2016 MS Project Pro 2016 MS Visio Pro 2016 Visual Studio Code Blender Gimp Maxima IntelliJ IDEA	Стол - 20 шт., стул - 20 шт., рабочее место сотрудника - 2 шт., персональный компьютер с выходом в интернет и обеспечением доступа в электронную информационно-образовательную среду академии – 17 шт., многофункциональное устройство – 2 шт.

		PyCharm Community Edition Adobe Reader DC MS Office Standart 2007 Windows 10 Pro	
235	Аудитория (защищаемое помещение) для проведения учебных занятий, с информацией ограниченного доступа, не содержащей сведений, составляющих государственную тайну	7-Zip Яндекс Браузер Mozilla Firefox LibreOffice	Стол – 8 шт., стул - 20 шт., рабочее место преподавателя – 1 шт., мультимедийный проектор (переносной) – 1 шт., переносной ноутбук – 1 шт., технические средства защиты

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

В соответствии с требованиями ФГОС ВО по направлению подготовки реализация компетентностного подхода предусматривает использование в учебном процессе активных и интерактивных форм проведения занятий (разбор конкретных задач, проведение блиц-опросов, исследовательские работы) в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.
Лекционные занятия дополняются ПЗ и различными формами СРС с учебной и научной литературой В процессе такой работы студенты приобретают навыки «глубокого чтения» - анализа и интерпретации текстов по методологии и методике дисциплины.
Учебный материал по дисциплине «Комплексная защита объектов информатизации». разделен на логически завершенные части (модули), после изучения, которых предусматривается аттестация в форме письменных тестов, контрольных работ.
Работы оцениваются в баллах, сумма которых дает рейтинг каждого обучающегося. В баллах оцениваются не только знания и навыки обучающихся, но и их творческие возможности: активность, неординарность решений поставленных проблем. Каждый модуль учебной дисциплины включает обязательные виды работ – лекции, ПЗ, различные виды СРС (выполнение домашних заданий по решению задач, подготовка к лекциям и практическим занятиям).
Форма текущего контроля знаний – работа студента на практическом занятии, опрос. Форма промежуточных аттестаций – контрольная работа в аудитории, домашняя работа. Итоговая форма контроля знаний по модулям – контрольная работа с задачами по материалу модуля.
Методические указания по выполнению всех видов учебной работы размещены в электронной образовательной среде академии.
Методические указания и материалы по видам учебных занятий по дисциплине:
Вид учебных занятий, работ - Организация деятельности обучающегося
Лекция - Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения, отмечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначить вопросы, термины, материал, который вызывает трудности, попытаться найти ответ в рекомендуемой литературе, если самостоятельно не удаётся разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии.
Практические занятия - Конспектирование источников. Работа с конспектом лекций, подготовка ответов к контрольным вопросам, просмотр рекомендуемой литературы, работа с текстом. Выполнение практических задач в инструментальных средах. Выполнение проектов. Решение расчётно-графических заданий, решение задач по алгоритму и др.
Самостоятельная работа - Знакомство с основной и дополнительной литературой, включая справочные издания, зарубежные источники, конспект основных положений, терминов, сведений, требующихся для запоминания и являющихся основополагающими в этой теме. Составление аннотаций к прочитанным литературным источникам и др

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ОБУЧАЮЩИМСЯ ПО ВЫПОЛНЕНИЮ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

Методические указания по выполнению самостоятельной работы по дисциплине «Комплексная защита объектов информатизации».
Формой осуществления контроля выполнения самостоятельной работы является подготовки рефератов на актуальные темы,
т. е. изучение с помощью научных методов явлений и процессов, анализа влияния на них различных факторов, а также, изучение взаимодействия между явлениями, с целью получения убедительно доказанных и полезных для науки и практики решений с максимальным эффектом.
Цель реферата – определение конкретного объекта и всестороннее, достоверное изучение его структуры, характеристик, связей на основе разработанных в науке принципов и методов познания, а также получение полезных для деятельности человека результатов, внедрение в производство с дальнейшим эффектом.
Основой разработки каждой темы является методология, т. е. совокупность методов, способов, приемов и их определенная последовательность, принятая при разработке научного исследования. В конечном счете, методология – это схема, план решения поставленной научно исследовательской задачи.

Процесс подготовки реферата состоит из следующих основных этапов:
1. Выбор темы и обоснование ее актуальности.
2. Составление библиографии, ознакомление с законодательными актами, нормативными документами и другими источниками, относящимися к теме проекта (работы).
3. Разработка алгоритма исследования, формирование требований к исходным данным, выбор методов и инструментальных
средств анализа.
4. Сбор фактического материала.
5. Обработка и анализ полученной информации с применением современных методов анализа.
6. Формулировка выводов и выработка рекомендаций.
7. Оформление работы в соответствии с установленными требованиями