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.03
Системы охраны и инженерной защиты информации
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 **4 ЗЕТ**

Часов по учебному плану 144
в том числе:
аудиторные занятия 80
самостоятельная работа 28
контактная работа во время промежуточной аттестации (ИКР) 0
часов на контроль 34,7

Виды контроля в семестрах:
экзамены 6

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**6 (3.2)**		Итого	
Недель	16 1/6			
Вид занятий	УП	РП	УП	РП
Лекции	32	32	32	32
Практические	48	48	48	48
Контактная работа на аттестации (в период экз. сессий)	0,3	0,3	0,3	0,3
Консультации перед экзаменом	1	1	1	1
Итого ауд.	80	80	80	80
Контактная работа	81,3	81,3	81,3	81,3
Сам. работа	28	28	28	28
Часы на контроль	34,7	34,7	34,7	34,7
Итого	144	144	144	144

Программу составил(и):
старший преподаватель, Алеферова В.В.

Рецензент(ы):
д.т.н., Профессор кафедры информатики и вычислительной техники КубГТУ, Хисамов Ф.Г.;директор АО «ЮГ-СИСТЕМА ПЛЮС», Глебов О.В.

Рабочая программа дисциплины
Системы охраны и инженерной защиты информации

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	Целью преподавания дисциплины «Системы охраны и инженерной защиты
1.2	информации» является ознакомление студентов с источниками и носителями
1.3	информации, изучение физических принципов возникновения технических
1.4	каналов утечки информации, способов и методик их выявления, оценки степени
1.5	опасности, методов и средств защиты.

Задачи: получить знания о демаскирующих признаках объектов;
 получить знания о технических каналах утечки информации и методиках их выявления;
 получить знания о методах защиты информации от утечек по радиоканалу;
 получить знания о методах защиты информации от утечек по виброакустическому каналу;
 получить знания о методах защиты информации от утечек по каналу ПЭМИН;
 получить знания о методах защиты информации от утечек по оптическому каналу;
 получить знания о средствах и охраны и методах их применения на объектах информатизации;
 получить навыки по разработке и проектированию обустройства помещений объектов с повышенными требованиями к инженерно-технической защите.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.В
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Безопасность систем баз данных
2.1.2	Экономика защиты информации
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Методы защиты программного обеспечения
2.2.2	Выполнение и защита выпускной квалификационной работы
2.2.3	Защита информационных процессов в компьютерных системах
2.2.4	Производственная практика: Технологическая практика
2.2.5	Производственная практика: Преддипломная практика
2.2.6	Комплексная защита объектов информатизации

3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ, ИНДИКАТОРЫ ИХ ДОСТИЖЕНИЯ и планируемые результаты обучения	
УК-3: Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде	
УК-3.1: Определяет свою роль в команде, исходя из стратегии сотрудничества для достижения поставленной цели	
Знать	
Уровень 1	Минимальный необходимый уровень знаний пределяет свою роль в команде, исходя из стратегии сотрудничества для достижения поставленной цели
Уровень 2	Уровень знаний Определяет свою роль в команде, исходя из стратегии сотрудничества для достижения поставленной цели в объёме, соответствующем программе подготовки, допущено несколько негрубых ошибок
Уровень 3	Уровень знаний Определяет свою роль в команде, исходя из стратегии сотрудничества для достижения поставленной цели в объёме, соответствующем программе подготовки, без ошибок
УК-3.2: При реализации своей роли в команде учитывает особенности поведения других членов команды	
Уметь	
Уровень 1	Продемонстрированы основные умения реализации своей роли в команде учитывает особенности поведения других членов команды, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме
Уровень 2	Продемонстрированы все основные умения реализации своей роли в команде учитывает особенности поведения других членов команды, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объёме, но некоторые с недочётами
Уровень 3	Продемонстрированы все основные умения реализации своей роли в команде учитывает особенности поведения других членов команды, решены все основные задачи с отдельными несущественными недочётами, выполнены все задания в полном объёме
УК-3.3: Анализирует возможные последствия личных действий и планирует свои действия для достижения заданного результата	

Владеть	
Уровень 1	Имеется минимальный набор навыков для анализа возможных последствий личных действий и планирования своих действий для достижения заданного результата с негрубыми ошибками и некоторыми недочётами
Уровень 2	Продемонстрированы базовые навыки для анализа возможных последствий личных действий и планирования своих действий для достижения заданного результата с некоторыми недочётами
Уровень 3	Продемонстрированы навыки для анализа возможных последствий личных действий и планирования своих действий для достижения заданного результата без ошибок и недочётов
УК-3.4: Осуществляет обмен информацией, знаниями и опытом с членами команды, оценивает идеи других членов команды для достижения поставленной цели	
Знать	
Уровень 1	Минимальный необходимый уровень знаний Осуществляет обмен информацией, знаниями и опытом с членами команды, оценивает идеи других членов команды для достижения поставленной цели
Уровень 2	Уровень знаний Осуществляет обмен информацией, знаниями и опытом с членами команды, оценивает идеи других членов команды для достижения поставленной цели в объёме, соответствующем программе подготовки, допущено несколько негрубых ошибок
Уровень 3	Уровень знаний Осуществляет обмен информацией, знаниями и опытом с членами команды, оценивает идеи других членов команды для достижения поставленной цели в объёме, соответствующем программе подготовки, без ошибок
Уметь	
Уровень 1	Продемонстрированы основные умения осуществлять обмен информацией, знаниями и опытом с членами команды, оценивает идеи других членов команды для достижения поставленной цели, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме
Уровень 2	Продемонстрированы все основные умения осуществлять обмен информацией, знаниями и опытом с членами команды, оценивает идеи других членов команды для достижения поставленной цели, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объёме, но некоторые с недочётами
Уровень 3	Продемонстрированы все основные умения осуществлять обмен информацией, знаниями и опытом с членами команды, оценивает идеи других членов команды для достижения поставленной цели, решены все основные задачи с отдельными несущественными недочётами, выполнены все задания в полном объёме
Владеть	
Уровень 1	Имеется минимальный набор навыков Осуществляет обмен информацией, знаниями и опытом с членами команды, оценивает идеи других членов команды для достижения поставленной цели с негрубыми ошибками и некоторыми недочётами
Уровень 2	Продемонстрированы базовые навыки Осуществляет обмен информацией, знаниями и опытом с членами команды, оценивает идеи других членов команды для достижения поставленной цели с некоторыми недочётами
Уровень 3	Продемонстрированы навыки Осуществляет обмен информацией, знаниями и опытом с членами команды, оценивает идеи других членов команды для достижения поставленной цели без ошибок и недочётов
УК-3.5: Соблюдает установленные нормы и правила командной работы, несет личную ответственность за общий результат	
Знать	
Уровень 1	Минимальный необходимый уровень Соблюдает установленные нормы и правила командной работы, несет личную ответственность за общий результат
Уровень 2	Уровень знаний Соблюдает установленные нормы и правила командной работы, несет личную ответственность за общий результат в объёме, соответствующем программе подготовки, допущено несколько негрубых ошибок
Уровень 3	Уровень знаний Соблюдает установленные нормы и правила командной работы, несет личную ответственность за общий результат в объёме, соответствующем программе подготовки, без ошибок
Уметь	
Уровень 1	Продемонстрированы основные умения Соблюдает установленные нормы и правила командной работы, несет личную ответственность за общий результат, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме
Уровень 2	Продемонстрированы все основные умения Соблюдает установленные нормы и правила командной работы, несет личную ответственность за общий результат, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объёме, но некоторые с недочётами
Уровень 3	Продемонстрированы все основные умения Соблюдает установленные нормы и правила командной работы, несет личную ответственность за общий результат, решены все основные задачи с отдельными несущественными недочётами, выполнены все задания в полном объёме
Владеть	
Уровень 1	Имеется минимальный набор навыков соблюдения установленных норм и правил командной работы, несет личную ответственность за общий результат с негрубыми ошибками и некоторыми недочётами
Уровень 2	Продемонстрированы базовые навыки соблюдения установленных норм и правил командной работы, несет личную ответственность за общий результат с некоторыми недочётами

Уровень 3	Продемонстрированы навыки соблюдения установленных норм и правил командной работы, несет личную ответственность за общий результат без ошибок и недочётов

ПК-2: Способен реализовывать политики безопасности с использованием инструментальных средств обеспечения информационной безопасности	
ПК-2.1: Формулирует критерии безопасности обработки информации в автоматизированных системах	
Знать	
Уровень 1	Минимальный необходимый уровень знаний формирования критериев безопасности обработки информации в автоматизированных системах
Уровень 2	Уровень знаний формирования критериев безопасности обработки информации в автоматизированных системах в объёме, соответствующем программе подготовки, допущено несколько негрубых ошибок
Уровень 3	Уровень знаний формирования критериев безопасности обработки информации в автоматизированных системах в объёме, соответствующем программе подготовки, без ошибок
ПК-2.2: Выполняет мероприятия для реализации политики информационной безопасности	
Уметь	
Уровень 1	Продемонстрированы основные умения выполнения мероприятий для реализации политики информационной безопасности, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме
Уровень 2	Продемонстрированы все основные умения выполнения мероприятий для реализации политики информационной безопасности, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объёме, но некоторые с недочётами
Уровень 3	Продемонстрированы все основные умения выполнения мероприятий для реализации политики информационной безопасности, решены все основные задачи с отдельными несущественными недочётами, выполнены все задания в полном объёме
ПК-2.3: Определяет состав средств, необходимый для управления автоматизированными системами и средствами их защиты от НСД	
Владеть	
Уровень 1	Имеется минимальный набор навыков определения состава средств, необходимых для управления автоматизированными системами и средствами их защиты от НСД с негрубыми ошибками и некоторыми недочётами
Уровень 2	Продемонстрированы базовые навыки определения состава средств, необходимых для управления автоматизированными системами и средствами их защиты от НСД с некоторыми недочётами
Уровень 3	Продемонстрированы навыки определения состава средств, необходимых для управления автоматизированными системами и средствами их защиты от НСД без ошибок и недочётов
ПК-2.4: Определяет порядок настройки технических средств для управления автоматизированными системами и средствами их защиты от НСД	
Знать	
Уровень 1	Минимальный необходимый уровень знаний определения порядка настройки технических средств для управления автоматизированными системами и средствами их защиты от НСД
Уровень 2	Уровень знаний определения порядка настройки технических средств для управления автоматизированными системами и средствами их защиты от НСД в объёме, соответствующем программе подготовки, допущено несколько негрубых ошибок
Уровень 3	Уровень знаний определения порядка настройки технических средств для управления автоматизированными системами и средствами их защиты от НСД в объёме, соответствующем программе подготовки, без ошибок
Уметь	
Уровень 1	Продемонстрированы основные умения Определяет порядок настройки технических средств для управления автоматизированными системами и средствами их защиты от НСД , решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме
Уровень 2	Продемонстрированы все основные умения Определяет порядок настройки технических средств для управления автоматизированными системами и средствами их защиты от НСД, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объёме, но некоторые с недочётами
Уровень 3	Продемонстрированы все основные Определяет порядок настройки технических средств для управления автоматизированными системами и средствами их защиты от НСД, решены все основные задачи с отдельными несущественными недочётами, выполнены все задания в полном объёме
Владеть	
Уровень 1	Имеется минимальный набор навыков Определяет порядок настройки технических средств для управления автоматизированными системами и средствами их защиты от НСД с негрубыми ошибками и некоторыми недочётами
Уровень 2	Продемонстрированы базовые навыки Определяет порядок настройки технических средств для управления автоматизированными системами и средствами их защиты от НСД с некоторыми недочётами
Уровень 3	Продемонстрированы навыки Определяет порядок настройки технических средств для управления автоматизированными системами и средствами их защиты от НСД без ошибок и недочётов

ПК-2.5: Устанавливает программное обеспечение в соответствии с требованиями по защите информации	
Знать	
Уровень 1	Минимальный необходимый уровень знаний Устанавливает программное обеспечение в соответствии с требованиями по защите информации
Уровень 2	Уровень знаний Устанавливает программное обеспечение в соответствии с требованиями по защите информации в объёме, соответствующем программе подготовки, допущено несколько негрубых ошибок
Уровень 3	Уровень знаний Устанавливает программное обеспечение в соответствии с требованиями по защите информации в объёме, соответствующем программе подготовки, без ошибок
Уметь	
Уровень 1	Продемонстрированы основные умения установки программного обеспечения в соответствии с требованиями по защите информации, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме
Уровень 2	Продемонстрированы все основные умения установки программного обеспечения в соответствии с требованиями по защите информации, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объёме, но некоторые с недочётами
Уровень 3	Продемонстрированы все основные умения установки программного обеспечения в соответствии с требованиями по защите информации, решены все основные задачи с отдельными несущественными недочётами, выполнены все задания в полном объёме
Владеть	
Уровень 1	Имеется минимальный набор навыков Устанавливает программное обеспечение в соответствии с требованиями по защите информации с негрубыми ошибками и некоторыми недочётами
Уровень 2	Продемонстрированы базовые навыки Устанавливает программное обеспечение в соответствии с требованиями по защите информации с некоторыми недочётами
Уровень 3	Продемонстрированы навыки Устанавливает программное обеспечение в соответствии с требованиями по защите информации без ошибок и недочётов

ПК-9: Способен организовывать работы по обеспечению информационной безопасности в автоматизированных системах	
ПК-9.1: Формулирование правил работы персонала со средствами защиты информации	
Знать	
Уровень 1	Минимальный необходимый уровень знаний формулирования правил работы персонала со средствами защиты информации
Уровень 2	Уровень знаний формулирования правил работы персонала со средствами защиты информации в объёме, соответствующем программе подготовки, допущено несколько негрубых ошибок
Уровень 3	Уровень знаний формулирования правил работы персонала со средствами защиты информации в объёме, соответствующем программе подготовки, без ошибок
ПК-9.2: Распределяет обязанности и полномочия персонала, обслуживающего защищённую автоматизированную систему	
Уметь	
Уровень 1	Продемонстрированы основные умения формулирования правил работы персонала со средствами защиты информации, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме
Уровень 2	Продемонстрированы все основные умения формулирования правил работы персонала со средствами защиты информации, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объёме, но некоторые с недочётами
Уровень 3	Продемонстрированы все основные умения формулирования правил работы персонала со средствами защиты информации, решены все основные задачи с отдельными несущественными недочётами, выполнены все задания в полном объёме
ПК-9.3: Сопоставляет результат работы персонала, обслуживающего защищённую автоматизированную систему, с целевыми показателями функционирования службы защиты информации	
Владеть	
Уровень 1	Имеется минимальный набор навыков сопоставления результатов работы персонала, обслуживающего защищённую автоматизированную систему, с целевыми показателями функционирования службы защиты информации с негрубыми ошибками и некоторыми недочётами
Уровень 2	Продемонстрированы базовые навыки сопоставления результатов работы персонала, обслуживающего защищённую автоматизированную систему, с целевыми показателями функционирования службы защиты информации с некоторыми недочётами
Уровень 3	Продемонстрированы навыки сопоставления результатов работы персонала, обслуживающего защищённую автоматизированную систему, с целевыми показателями функционирования службы защиты информации без ошибок и недочётов

ПК-10: Способен собирать, анализировать и систематизировать информацию по зафиксированным инцидентам информационной безопасности

ПК-10.1: Соотносит инциденты информационной безопасности с характеристиками систем и средств защиты информации	
Знать	
Уровень 1	Минимальный необходимый уровень знаний соотнесения инцидентов информационной безопасности с характеристиками систем и средств защиты информации
Уровень 2	Уровень знаний соотнесения инцидентов информационной безопасности с характеристиками систем и средств защиты информации в объёме, соответствующем программе подготовки, допущено несколько негрубых ошибок
Уровень 3	Уровень знаний соотнесения инцидентов информационной безопасности с характеристиками систем и средств защиты информации в объёме, соответствующем программе подготовки, без ошибок
ПК-10.2: Обосновывает необходимость модернизации системы защиты информации автоматизированной системы	
Уметь	
Уровень 1	Продемонстрированы основные умения обосновывания необходимости модернизации системы защиты информации автоматизированной системы, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме
Уровень 2	Продемонстрированы все основные умения обосновывания необходимости модернизации системы защиты информации автоматизированной системы, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объёме, но некоторые с недочётами
Уровень 3	Продемонстрированы все основные умения обосновывания необходимости модернизации системы защиты информации автоматизированной системы, решены все основные задачи с отдельными несущественными недочётами, выполнены все задания в полном объёме
ПК-10.3: Формулирует правила применения мер защиты информации, направленные на устранение причин возникновения инцидентов информационной безопасности	
Владеть	
Уровень 1	Имеется минимальный набор навыков формулирования правил, применения мер защиты информации, направленные на устранение причин возникновения инцидентов информационной безопасности с негрубыми ошибками и некоторыми недочётами
Уровень 2	Продемонстрированы базовые навыки формулирования правил, применения мер защиты информации, направленные на устранение причин возникновения инцидентов информационной безопасности с некоторыми недочётами
Уровень 3	Продемонстрированы навыки формулирования правил, применения мер защиты информации, направленные на устранение причин возникновения инцидентов информационной безопасности без ошибок и недочётов
ПК-10.4: Формулирует правила протоколирования результатов мониторинга безопасности автоматизированных систем	
Знать	
Уровень 1	Минимальный необходимый уровень знаний формулирования правил протоколирования результатов мониторинга безопасности автоматизированных систем
Уровень 2	Уровень знаний формулирования правил протоколирования результатов мониторинга безопасности автоматизированных систем в объёме, соответствующем программе подготовки, допущено несколько негрубых ошибок
Уровень 3	Уровень знаний формулирования правил протоколирования результатов мониторинга безопасности автоматизированных систем в объёме, соответствующем программе подготовки, без ошибок
Уметь	
Уровень 1	Продемонстрированы основные умения Формулирует правила протоколирования результатов мониторинга безопасности автоматизированных систем, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме
Уровень 2	Продемонстрированы все основные умения Формулирует правила протоколирования результатов мониторинга безопасности автоматизированных систем, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объёме, но некоторые с недочётами
Уровень 3	Продемонстрированы все основные умения Формулирует правила протоколирования результатов мониторинга безопасности автоматизированных систем, решены все основные задачи с отдельными несущественными недочётами, выполнены все задания в полном объёме
Владеть	
Уровень 1	Имеется минимальный набор навыков Формулирует правила протоколирования результатов мониторинга безопасности автоматизированных систем с негрубыми ошибками и некоторыми недочётами
Уровень 2	Продемонстрированы базовые навыки Формулирует правила протоколирования результатов мониторинга безопасности автоматизированных систем с некоторыми недочётами
Уровень 3	Продемонстрированы навыки Формулирует правила протоколирования результатов мониторинга безопасности автоматизированных систем без ошибок и недочётов

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	Задачи курса «Системы охраны и инженерной защиты информации» /Лек/	6	4	УК-3.1 УК-3.2 УК-3.3 УК-3.4 ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4 ПК-2.5 ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	
1.2	Задачи курса «Системы охраны и инженерной защиты информации» /Ср/	6	4	УК-3.1 УК-3.2 УК-3.3 УК-3.4 ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4 ПК-2.5 ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	
1.3	Задачи курса «Системы охраны и инженерной защиты информации» /Пр/	6	4	УК-3.1 УК-3.2 УК-3.3 УК-3.4 ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4 ПК-2.5 ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	
1.4	Угрозы информационной безопасности информации и объекты защиты /Лек/	6	2	УК-3.1 УК-3.2 УК-3.3 УК-3.4 ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4 ПК-2.5 ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	
1.5	Угрозы информационной безопасности информации и объекты защиты /Ср/	6	2	УК-3.1 УК-3.2 УК-3.3 УК-3.4 ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4 ПК-2.5 ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	

1.6	Угрозы информационной безопасности информации и объекты защиты /Пр/	6	4	УК-3.1 УК-3.2 УК-3.3 УК-3.4 ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4 ПК-2.5 ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	
1.7	Демаскирующие признаки объектов защиты. Классификация демаскирующих признаков /Лек/	6	2	УК-3.1 УК-3.2 УК-3.3 УК-3.4 ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4 ПК-2.5 ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	
1.8	Демаскирующие признаки объектов защиты. Классификация демаскирующих признаков /Ср/	6	2	УК-3.1 УК-3.2 УК-3.3 УК-3.4 ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4 ПК-2.5 ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	
1.9	Демаскирующие признаки объектов защиты. Классификация демаскирующих признаков /Пр/	6	4	УК-3.1 УК-3.2 УК-3.3 УК-3.4 ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4 ПК-2.5 ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	
1.10	Источники и носители информации /Лек/	6	2	УК-3.1 УК-3.2 УК-3.3 УК-3.4 ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4 ПК-2.5 ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	

1.11	Источники и носители информации /Ср/	6	2	УК-3.1 УК-3.2 УК-3.3 УК-3.4 ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4 ПК-2.5 ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	
1.12	Источники и носители информации /Пр/	6	4	УК-3.1 УК-3.2 УК-3.3 УК-3.4 ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4 ПК-2.5 ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	
1.13	Принципы и способы добывания информации /Лек/	6	2	УК-3.1 УК-3.2 УК-3.3 УК-3.4 ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4 ПК-2.5 ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	
1.14	Принципы и способы добывания информации /Ср/	6	2	УК-3.1 УК-3.2 УК-3.3 УК-3.4 ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4 ПК-2.5 ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	
1.15	Принципы и способы добывания информации /Пр/	6	4	УК-3.1 УК-3.2 УК-3.3 УК-3.4 ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4 ПК-2.5 ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	

1.16	Основы противодействия техническим средствам разведки /Лек/	6	2	УК-3.1 УК-3.2 УК-3.3 УК-3.4 ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4 ПК-2.5 ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	
1.17	Основы противодействия техническим средствам разведки /Ср/	6	2	УК-3.1 УК-3.2 УК-3.3 УК-3.4 ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4 ПК-2.5 ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	
1.18	Основы противодействия техническим средствам разведки /Пр/	6	4	УК-3.1 УК-3.2 УК-3.3 УК-3.4 ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4 ПК-2.5 ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	
1.19	Технические каналы утечки информации (электромагнитные каналы, электрические каналы, параметрические каналы, вибрационные каналы) /Лек/	6	2	УК-3.1 УК-3.2 УК-3.3 УК-3.4 ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4 ПК-2.5 ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	
1.20	Технические каналы утечки информации (электромагнитные каналы, электрические каналы, параметрические каналы, вибрационные каналы) /Ср/	6	2	УК-3.1 УК-3.2 УК-3.3 УК-3.4 ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4 ПК-2.5 ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	

1.21	Технические каналы утечки информации (электромагнитные каналы, электрические каналы, параметрические каналы, вибрационные каналы) /Пр/	6	4	УК-3.1 УК-3.2 УК-3.3 УК-3.4 ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4 ПК-2.5 ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	
1.22	Каналы утечки речевой информации /Лек/	6	2	УК-3.1 УК-3.2 УК-3.3 УК-3.4 ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4 ПК-2.5 ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	
1.23	Каналы утечки речевой информации /Ср/	6	2	УК-3.1 УК-3.2 УК-3.3 УК-3.4 ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4 ПК-2.5 ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	
1.24	Каналы утечки речевой информации /Пр/	6	4	УК-3.1 УК-3.2 УК-3.3 УК-3.4 ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4 ПК-2.5 ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	
1.25	Каналы утечки информации при передаче по каналам связи /Лек/	6	2	УК-3.1 УК-3.2 УК-3.3 УК-3.4 ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4 ПК-2.5 ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	

1.26	Каналы утечки информации при передаче по каналам связи /Ср/	6	2	УК-3.1 УК-3.2 УК-3.3 УК-3.4 ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4 ПК-2.5 ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	
1.27	Каналы утечки информации при передаче по каналам связи /Ср/	6	4	УК-3.1 УК-3.2 УК-3.3 УК-3.4 ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4 ПК-2.5 ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	
1.28	Технические каналы утечки видовой информации /Лек/	6	2	УК-3.1 УК-3.2 УК-3.3 УК-3.4 ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4 ПК-2.5 ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	
1.29	Технические каналы утечки видовой информации /Ср/	6	2	УК-3.1 УК-3.2 УК-3.3 УК-3.4 ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4 ПК-2.5 ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	
1.30	Технические каналы утечки видовой информации /Пр/	6	4	УК-3.1 УК-3.2 УК-3.3 УК-3.4 ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4 ПК-2.5 ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	

1.31	Несанкционированный доступ к информации, обрабатываемой средствами вычислительной техники /Лек/	6	4	УК-3.1 УК-3.2 УК-3.3 УК-3.4 ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4 ПК-2.5 ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	
1.32	Несанкционированный доступ к информации, обрабатываемой средствами вычислительной техники /Ср/	6	2	УК-3.1 УК-3.2 УК-3.3 УК-3.4 ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4 ПК-2.5 ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	
1.33	Несанкционированный доступ к информации, обрабатываемой средствами вычислительной техники /Пр/	6	6	УК-3.1 УК-3.2 УК-3.3 УК-3.4 ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4 ПК-2.5 ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	
1.34	Звукоизоляция помещений /Лек/	6	6	УК-3.1 УК-3.2 УК-3.3 УК-3.4 ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4 ПК-2.5 ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	
1.35	Звукоизоляция помещений /Пр/	6	6	УК-3.1 УК-3.2 УК-3.3 УК-3.4 ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4 ПК-2.5 ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	
	Раздел 2. Промежуточная аттестация					

2.1	Экзамен /КАЭ/	6	0,3	УК-3.1 УК-3.2 УК-3.3 УК-3.4 ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4 ПК-2.5 ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	
2.2	Консультация /Консл/	6	1	УК-3.1 УК-3.2 УК-3.3 УК-3.4 ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4 ПК-2.5 ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

5.1. Контрольные вопросы и задания

1.Понятие информации. Виды представления и классификация информации.
2. Понятия безопасности и системы безопасности информации. Системный подход к защите информации.
3. Угрозы конфиденциальной информации и их классификация.
4. Источники угроз безопасности информации, их классификация и ранжирование.
5. Уязвимости безопасности информации, их классификация и ранжирование.
6. Действия, приводящие к неправомерному овладению конфиденциальной информацией.
7. Правовая и организационная защита информации.
8. Инженерно-инженерно- техническая защита информации.
9. Классификация и общая характеристика каналов утечки информации.
10.Технические каналы утечки информации и их образование.
11. Классификация и характеристика каналов утечки речевой информации.
12.Технические каналы утечки речевой информации и методы ее съема.
13. Методы дистанционного проникновения в помещение для скрытого съема аудио - и видеоинформации.
14.Технические средства съема аудиоинформации. Микрофоны и их виды.
15.Методы съема информации в телефонных линиях связи.
16.Технические средства съема видеоинформации и их общая характеристика.
17.Методы и средства съема информации по радиоканалу.
18.Методы и средства съема информации телевизионной и вычислительной техники.
19.Методы и средства съема информации в высокочастотных и волоконно- оптическихкабелях.
20. Защита речевой информации с помощью маскирующих сигналов.
21. Системы виброакустического зашумления.
22. Защита речевой информации от лазерного съема.
23.Методы и средства обнаружения радиозакладных устройств. Индикаторы поля, панорамные сканирующие приемники, аппаратно-программные комплексы.
24.Методы и средства обнаружения радиозакладных устройств. Обнаружители диктофонов и нелинейные радиолокаторы.
25.Звукоизоляция помещений.
26.Общие принципы защиты телефонных линий связи. Методы и средства пассивной защиты.
27.Методы подавления телефонных закладных устройств.
28.Методы и средства обнаружения и противодействия в телефонных линиях связи.
29.Общая характеристика методов защиты информации от утечки по электромагнитным каналам.
30.Защита линий связи. Защита информации от утечки в волоконно- оптических линиях связи.

5.2. Темы письменных работ

Курсовая работа не предусмотрена

5.3. Фонд оценочных средств

1. Конечное множество используемых для кодирования информации знаков называется
алфавитом
кодом
ключом
шифром

2. Математические методы нарушения конфиденциальности и аутентичности информации без знания ключей объединяет
криптоанализ
криптография
стеганография
криптология

3. Модели политики безопасности на основе анализа угроз системе исследуют вероятность преодоления системы защиты
за определенное время
фиксированными затратами
ограниченной компетенцией злоумышленника
фиксированным ресурсом

4. Надежность СЗИ определяется
самым слабым звеном
количеством отраженных атак
усредненным показателем
самым сильным звеном

5. Наименее затратный криптоанализ для криптоалгоритма RSA
разложение числа на простые множители
перебор по всему ключевому пространству
перебор по выборочному ключевому пространству
разложение числа на сложные множители

6. Недостатком дискретных моделей политики безопасности является
статичность
необходимость дополнительного обучения персонала
изначальное допущение вскрываемости системы
сложный механизм реализации

7. Недостатком модели политики безопасности на основе анализа угроз системе является
изначальное допущение вскрываемости системы
необходимость дополнительного обучения персонала
сложный механизм реализации
статичность

8. Нормативный документ, регламентирующий все аспекты безопасности продукта информационных технологий, называется
профилем защиты
профилем безопасности
стандартом безопасности
системой защиты

9. Обеспечением скрытности информации в информационных массивах занимается
стеганография
криптоанализ
криптология
криптография

10. Основным положением модели системы безопасности с полным перекрытием является наличие на каждом пути проникновения в систему
хотя бы одного средства безопасности
аудита
пароля
всех средств безопасности

11. Первым этапом разработки системы защиты ИС является
анализ потенциально возможных угроз информации
оценка возможных потерь

стандартизация программного обеспечения
изучение информационных потоков

12. По документам ГТК количество классов защищенности СВТ от НСД к информации
6
9
8
7

13. По документам ГТК самый низкий класс защищенности СВТ от НСД к информации
6
9
0
1

14. Политика информационной безопасности – это
совокупность законов, правил, определяющих управленческие и проектные решения в области защиты информации
стандарс безопасности
профиль защиты
итоговый документ анализа рисков

15. При избирательной политике безопасности в матрице доступа объекту системы соответствует
строка
прямоугольная область
ячейка
столбец

5.4. Перечень видов оценочных средств

Задания со свободно конструируемым ответом (СКО) предполагает составление развернутого ответа на теоретический вопрос. Задание с выбором одного варианта ответа (ОВ, в задании данного типа предлагается несколько вариантов ответа, среди которых один верный. 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
Л1.3	Жук А.П., Жук Е.П.	Защита информации: Учебное пособие	Москва: Издательский Центр РИО□, 2021, URL: http://znanium.com/catalog/document?id=367588

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год
Л2.1	Москвитин Г. И.	Комплексная защита информации в организации: Монография	Москва: Русайнс, 2017, URL: https://book.ru/book/922538
Л2.2	Ищейнов В. Я.	Информационная безопасность и защита информации: словарь терминов и понятий: Словарь	Москва: Русайнс, 2019, URL: https://book.ru/book/932909

6.2. Электронные учебные издания и электронные образовательные ресурсы

Э1	Национальный открытый университет "ИНТУИТ". - Режим доступа: https://www.intuit.ru/studies/courses%20
Э2	Электронно-библиотечная система. - Режим доступа: http://znanium.com/%20
Э3	ЭИОС. - Режим доступа: http://eios.imsit.ru/
Э4	ЭБС Айбукс. - Режим доступа: http://www.ibooks.ru/
Э5	РПД. - Режим доступа: http://rpd.eios.imsit.ru:8080/RPD/Index/1636711/%20http://www.book.ru

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	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
113	Лаборатория технической защиты информации	Windows 10 Pro RUS 7-Zip Яндекс Браузер Mozilla Firefox LibreOffice LibreCAD 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 Traffic inspector Special Unlimited Ramus Educational Micro-Cap Evaluation vGate Secren Net Studio Secren Net LSP	Стол - 20 шт., стул - 21 шт., рабочее место преподавателя - 1 шт., доска учебная – 1 шт., персональный компьютер с выходом в интернет – 21 шт., интерактивная доска с проектором - 1 шт., многофункциональное устройство– 1 шт., комплект презентаций, лабораторные учебные макеты, аппаратные средства аутентификации пользователя, средства защиты информации от утечки по акустическому (виброакустическому) каналу и каналу побочных электромагнитных излучений и наводок, средства измерения параметров физических полей (электромагнитных излучений и наводок, акустических (виброакустических) колебаний и тд.), стенды физической защиты объектов информатизации оснащенными средствами контроля доступа системами видеонаблюдения и охраны объектов, соответствующее программное обеспечение, учебно-наглядные методические пособия, комплект оборудования Arduino - 3 шт., учебный комплект SDK 1.1s - 5 шт., комплект инструментов для сборки ПК - 12 шт., средства защиты информации от утечки по акустическому каналу, каналу побочных электромагнитных излучений и наводок, акустовибрационному и акустоэлектрическому каналам, техническими средствами контроля эффективности защиты информации от утечки по указанным каналам, антивирусные программные комплексы, аппаратные средства аутентификации пользователя, программно-аппаратные комплексы защиты информации, включающие в том числе средства криптографической защиты информации (средства анализа защищенности компьютерных сетей, аппаратно-программные средства управления доступом к данным, стенды, Сигурд-М19 (автоматизированная система оценки защищенности технических средств от утечки информации по каналу побочных электромагнитных излучений и наводок) – 1 шт., Шепот-М1 (автоматизированная система оценки защищенности выделенных помещений по виброакустическому каналу) – 1 шт.
121	Компьютерный класс	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	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

		Oracle VM VirtualBox StarUML V1 PostgreSQL IntelliJ IDEA PyCharm Community Edition Eclips Adobe Reader DC Arduino Software (IDE) NetBeans IDE ZEAL ARIS Express Archimate ПО ЛИНКО v8.2 демо-версия Klite Mega Codec Pack Ramus Educational Micro-Cap Evaluation gvSIG Desktop Python	
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 PyCharm Community Edition Adobe Reader DC MS Office Standart 2007 Windows 10 Pro	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.

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 «Системы охраны и инженерной защиты информации». 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 «Системы охраны и инженерной защиты информации».
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.