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.О.17
Основы информационной безопасности
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 **2 ЗЕТ**

Часов по учебному плану 72
в том числе:
аудиторные занятия 48
самостоятельная работа 23,8
контактная работа во время промежуточной аттестации (ИКР) 0

Виды контроля в семестрах:
зачеты с оценкой 2

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**2 (1.2)**		Итого	
Недель	16 1/6			
Вид занятий	УП	РП	УП	РП
Лекции	32	32	32	32
Практические	16	16	16	16
Контактная работа на аттестации	0,2	0,2	0,2	0,2
Итого ауд.	48	48	48	48
Контактная работа	48,2	48,2	48,2	48,2
Сам. работа	23,8	23,8	23,8	23,8
Итого	72	72	72	72

Программу составил(и):
ктн, доцент, Капустин С.А.

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

Рабочая программа дисциплины
Основы информационной безопасности

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	приобретение обучающимися знаний, навыков и умений, связанных с правовыми и программно-техническими методами защиты информации государственных и негосударственных организаций и учреждений

Задачи: систематизация теоретических знаний по обеспечению безопасности информации в системах управления, использующих современные информационные технологии;
выявление сущности, целей, задач и места методов и средств защиты информационных процессов в компьютерных системах в общей системе обеспечения безопасности информации на объектах информатизации;
изучение основных принципов применения методов и средств защиты информации при организации защиты информационных процессов в компьютерных системах;
изучение нормативно-руководящих документов, регламентирующих вопросы обеспечения безопасности информации в автоматизированных системах

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.О
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Информатика
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Учебная практика: Ознакомительная практика
2.2.2	Производственная практика: Эксплуатационная
2.2.3	Выполнение и защита выпускной квалификационной работы

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

УК-1: Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач

УК-1.1: Анализирует задачу, выделяя ее базовые составляющие

Знать

Уровень 1	Минимальный необходимый уровень знаний для анализа задачи, с выделением ее базовых составляющих
Уровень 2	Уровень знаний для анализа задачи, с выделением ее базовых составляющих в объёме, соответствующем программе подготовки, допущено несколько негрубых ошибок
Уровень 3	Уровень знаний для анализа задачи, с выделением ее базовых составляющих в объёме, соответствующем программе подготовки, без ошибок

УК-1.2: Определяет и ранжирует информацию, требуемую для решения поставленной задачи

Уметь

Уровень 1	Продемонстрированы основные умения определения и ранжирования информации, требуемой для решения поставленной задачи в рамках избранных видов профессиональной деятельности, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме
Уровень 2	Продемонстрированы все основные умения определения и ранжирования информации, требуемой для решения поставленной задачи в рамках избранных видов профессиональной деятельности, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объёме, но некоторые с недочётами
Уровень 3	Продемонстрированы все основные умения определения и ранжирования информации, требуемой для решения поставленной задачи в рамках избранных видов профессиональной деятельности, решены все основные задачи с отдельными несущественными недочётами, выполнены все задания в полном объёме

УК-1.3: Осуществляет поиск информации для решения поставленной задачи по различным типам запросов

Владеть

Уровень 1	Имеется минимальный набор навыков поиска информации для решения поставленной задачи по различным типам запросов с негрубыми ошибками и некоторыми недочётами
Уровень 2	Продемонстрированы базовые навыки поиска информации для решения поставленной задачи по различным типам запросов с некоторыми недочётами
Уровень 3	Продемонстрированы навыки поиска информации для решения поставленной задачи по различным типам запросов без ошибок и недочётов

ОПК-1: Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства;

ОПК-1.1: Классифицирует угрозы информационной безопасности в соответствии с нормативными документами

Знать

Уровень 1	Минимальный необходимый уровень знаний классификации угроз информационной безопасности в соответствии с нормативными документами

Уровень 2	Уровень знаний классификации угроз информационной безопасности в соответствии с нормативными документами в объёме, соответствующем программе подготовки, допущено несколько негрубых ошибок
Уровень 3	Уровень знаний классификации угроз информационной безопасности в соответствии с нормативными документами в объёме, соответствующем программе подготовки, без ошибок
ОПК-1.2: Оценивает угрозы информационной безопасности с точки зрения основных концепций национальной безопасности Российской Федерации	
Уметь	
Уровень 1	Продемонстрированы основные умения оценки угроз информационной безопасности с точки зрения основных концепций национальной безопасности Российской Федерации с негрубыми ошибками, выполнены все задания, но не в полном объёме
Уровень 2	Продемонстрированы все основные умения оценки угроз информационной безопасности с точки зрения основных концепций национальной безопасности Российской Федерации с негрубыми ошибками, выполнены все задания в полном объёме, но некоторые с недочётами
Уровень 3	Продемонстрированы все основные умения оценки угроз информационной безопасности с точки зрения основных концепций национальной безопасности Российской Федерации с отдельными несущественными недочётами, выполнены все задания в полном объёме
ОПК-1.3: Определяет угрозы информационной безопасности для различных систем	
Владеть	
Уровень 1	Имеется минимальный набор навыков определения угрозы информационной безопасности для различных систем с негрубыми ошибками и некоторыми недочётами
Уровень 2	Продемонстрированы базовые навыки определения угрозы информационной безопасности для различных систем с некоторыми недочётами
Уровень 3	Продемонстрированы навыки определения угрозы информационной безопасности для различных систем без ошибок и недочётов

ОПК-9: Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности;	
ОПК-9.1: Использует средства криптографической защиты информации в автоматизированных системах	
Знать	
Уровень 1	Минимальный необходимый уровень знаний средств криптографической защиты информации в автоматизированных системах
Уровень 2	Уровень знаний средств криптографической защиты информации в автоматизированных системах в объёме, соответствующем программе подготовки, допущено несколько негрубых ошибок
Уровень 3	Уровень знаний средств криптографической защиты информации в автоматизированных системах в объёме, соответствующем программе подготовки, без ошибок
ОПК-9.2: Решает задачи криптографической защиты информации с использованием блочных и поточных систем шифрования, криптографических систем с открытым ключом, криптографических хеш-функций и криптографических протоколов	
Уметь	
Уровень 1	Продемонстрированы основные умения решать задачи криптографической защиты информации с использованием блочных и поточных систем шифрования, криптографических систем с открытым ключом, криптографических хеш-функций и криптографических протоколов, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме
Уровень 2	Продемонстрированы все основные умения решать задачи криптографической защиты информации с использованием блочных и поточных систем шифрования, криптографических систем с открытым ключом, криптографических хеш-функций и криптографических протоколов, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объёме, но некоторые с недочётами
Уровень 3	Продемонстрированы все основные умения решать задачи криптографической защиты информации с использованием блочных и поточных систем шифрования, криптографических систем с открытым ключом, криптографических хеш-функций и криптографических протоколов, решены все основные задачи с отдельными несущественными недочётами, выполнены все задания в полном объёме
ОПК-9.3: Организует защиту информации от утечки по техническим каналам на объектах информатизации	
Владеть	
Уровень 1	Имеется минимальный набор навыков для организации защиты информации от утечки по техническим каналам на объектах информатизации с негрубыми ошибками и некоторыми недочётами
Уровень 2	Продемонстрированы базовые навыки для организации защиты информации от утечки по техническим каналам на объектах информатизации с некоторыми недочётами
Уровень 3	Продемонстрированы навыки для организации защиты информации от утечки по техническим каналам на объектах информатизации без ошибок и недочётов

ОПК-9.4: Оценивает угрозы информационной безопасности объекта информатизации	
Уметь	
Уровень 1	Продемонстрированы основные умения оценивать угрозы информационной безопасности объекта информатизации, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме
Уровень 2	Продемонстрированы все основные умения оценивать угрозы информационной безопасности объекта информатизации, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объёме, но некоторые с недочётами
Уровень 3	Продемонстрированы все основные умения оценивать угрозы информационной безопасности объекта информатизации, решены все основные задачи с отдельными несущественными недочётами, выполнены все задания в полном объёме
ОПК-9.5: Использует средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации	
Владеть	
Уровень 1	Имеется минимальный набор навыков использования средств защиты информации от утечки по техническим каналам и контроля эффективности защиты информации с негрубыми ошибками и некоторыми недочётами
Уровень 2	Продемонстрированы базовые навыки использования средств защиты информации от утечки по техническим каналам и контроля эффективности защиты информации с некоторыми недочётами
Уровень 3	Продемонстрированы навыки использования средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации 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. Информационная безопасность в системе национальной безопасности России					
1.1	Доктрина информационной безопасности Российской Федерации Основы информационной безопасности /Лек/	2	4	УК-1.1 УК-1.2 УК-1.3 ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11 Л1.12 Л1.13Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13 Л2.14 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
1.2	Государственная политика в области обеспечения безопасности автоматизированных систем управления Государственная политика Российской Федерации в области международной информационной безопасности Защита персональных данных Защита Государственной тайны /Пр/	2	8	УК-1.1 УК-1.2 УК-1.3 ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11 Л1.12 Л1.13Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13 Л2.14 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
1.3	Допуск к Государственной тайне /Лек/	2	4	УК-1.1 УК-1.2 УК-1.3 ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11 Л1.12 Л1.13Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13 Л2.14 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	

1.4	/Ср/	2	10	УК-1.1 УК-1.2 УК-1.3 ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11 Л1.12 Л1.13Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13 Л2.14 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
	Раздел 2. Информационная война, методы и средства ее ведения					
2.1	Методы и средства ведения информационной войны /Лек/	2	2	УК-1.1 УК-1.2 УК-1.3 ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11 Л1.12 Л1.13Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13 Л2.14 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
2.2	Сетецентрические войны Фейки /Пр/	2	2	УК-1.1 УК-1.2 УК-1.3 ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11 Л1.12 Л1.13Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13 Л2.14 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
2.3	/Ср/	2	2	УК-1.1 УК-1.2 УК-1.3 ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11 Л1.12 Л1.13Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13 Л2.14 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
	Раздел 3. Критерии защищенности компьютерных систем					
3.1	Стандарты информационной безопасности /Лек/	2	2	УК-1.1 УК-1.2 УК-1.3 ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11 Л1.12 Л1.13Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13 Л2.14 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
3.2	Угрозы безопасности информации Основные типы политики безопасности доступа к данным. Дискреционные и мандатные политики /Лек/	2	4	УК-1.1 УК-1.2 УК-1.3 ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11 Л1.12 Л1.13Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13 Л2.14 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	

3.3	Защита от НСД /Лек/	2	4	УК-1.1 УК-1.2 УК-1.3 ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11 Л1.12 Л1.13Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13 Л2.14 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
	Раздел 4. Защита информации, обрабатываемой в информационных системах					
4.1	Защита информации в ГИС Защита информации в КИИ /Лек/	2	4	УК-1.1 УК-1.2 УК-1.3 ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11 Л1.12 Л1.13Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13 Л2.14 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
4.2	Работа со средствами защиты информации /Пр/	2	4	УК-1.1 УК-1.2 УК-1.3 ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11 Л1.12 Л1.13Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13 Л2.14 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
4.3	Программно-аппаратная защита информации /Лек/	2	4	УК-1.1 УК-1.2 УК-1.3 ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11 Л1.12 Л1.13Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13 Л2.14 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
4.4	/Ср/	2	6	УК-1.1 УК-1.2 УК-1.3 ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11 Л1.12 Л1.13Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13 Л2.14 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
	Раздел 5. Защита АС и СВТ от внешнего электромагнитного воздействия					
5.1	Защита АС и СВТ от внешнего электромагнитного воздействия /Лек/	2	2	УК-1.1 УК-1.2 УК-1.3 ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11 Л1.12 Л1.13Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13 Л2.14 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	

5.2	Требования руководящих документов по защите от ПЭМИН /Пр/	2	2	УК-1.1 УК-1.2 УК-1.3 ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11 Л1.12 Л1.13Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13 Л2.14 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
5.3	/Ср/	2	3,8	УК-1.1 УК-1.2 УК-1.3 ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11 Л1.12 Л1.13Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13 Л2.14 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
5.4	DLP-системы. Заключение. /Лек/	2	2	УК-1.1 УК-1.2 УК-1.3 ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11 Л1.12 Л1.13Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13 Л2.14	
5.5	/Ср/	2	2	УК-1.1 УК-1.2 УК-1.3 ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11 Л1.12 Л1.13Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13 Л2.14	
	Раздел 6. Промежуточная аттестация					
6.1	Зачет /КА/	2	0,2	УК-1.1 УК-1.2 УК-1.3 ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5		

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

5.1. Контрольные вопросы и задания

Контрольные вопросы для проведения текущего контроля

1. Угроза информационной безопасности Российской Федерации

совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере

совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в сфере общества и государства

2. Информационная безопасность Российской Федерации

состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие

Российской Федерации, оборона и безопасность государства;
взаимоувязанные правовые, организационные, оперативно-разыскные, разведывательные, контрразведывательные, научно-технические, информационно-аналитические, кадровые, экономические и иные меры по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления;

3. Обеспечение информационной безопасности
осуществление взаимоувязанных правовых, организационных, оперативно-разыскных, разведывательных, контрразведывательных, научно-технических, информационно-аналитических, кадровых, экономических и иных мер по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления;

4. Силы обеспечения информационной безопасности
государственные органы, а также подразделения и должностные лица государственных органов, органов местного самоуправления и организаций, уполномоченные на решение в соответствии с законодательством Российской Федерации задач по обеспечению информационной безопасности;
правовые, организационные, технические и другие средства, используемые силами обеспечения информационной безопасности;
взаимоувязанные правовые, организационные, оперативно-разыскные, разведывательные, контрразведывательные, научно-технические, информационно-аналитические, кадровые, экономические и иные меры по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления;

5. Средства обеспечения информационной безопасности
правовые, организационные, технические и другие средства, используемые силами обеспечения информационной безопасности;
государственные органы, а также подразделения и должностные лица государственных органов, органов местного самоуправления и организаций, уполномоченные на решение в соответствии с законодательством Российской Федерации задач по обеспечению информационной безопасности;
взаимоувязанные правовые, организационные, оперативно-разыскные, разведывательные, контрразведывательные, научно-технические, информационно-аналитические, кадровые, экономические и иные меры по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления;

6. Система обеспечения информационной безопасности
совокупность сил обеспечения информационной безопасности, осуществляющих скоординированную и спланированную деятельность, и используемых ими средств обеспечения информационной безопасности;
взаимоувязанные правовые, организационные, оперативно-разыскные, разведывательные, контрразведывательные, научно-технические, информационно-аналитические, кадровые, экономические и иные меры по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления;
государственные органы, а также подразделения и должностные лица государственных органов, органов местного самоуправления и организаций, уполномоченные на решение в соответствии с законодательством Российской Федерации задач по обеспечению информационной безопасности;

7. Информационная инфраструктура Российской Федерации
совокупность объектов информатизации, информационных систем, сайтов в сети «Интернет» и сетей связи, расположенных на территории Российской Федерации, а также на территориях, находящихся под юрисдикцией Российской Федерации или используемых на основании международных договоров Российской Федерации.
совокупность объектов информатизации, глобальных информационных систем, государственных информационных систем, критических информационных инфраструктур, расположенных на территории Российской Федерации.

8. На каких принципах основывается деятельность государственных органов по обеспечению информационной безопасности?
законность общественных отношений в информационной сфере и правовое равенство всех участников таких отношений, основанные на конституционном праве граждан свободно искать, получать, передавать, производить и распространять информацию любым законным способом;
конструктивное взаимодействие государственных органов, организаций и граждан при решении задач по обеспечению информационной безопасности;
соблюдение баланса между потребностью граждан в свободном обмене информацией и ограничениями, связанными с необходимостью обеспечения национальной безопасности, в том числе в информационной сфере;
создание международно-правовых механизмов, учитывающих специфику информационных технологий, в целях предотвращения и урегулирования межгосударственных конфликтов в информационном пространстве;
продвижение в рамках деятельности международных организаций позиции Российской Федерации, предусматривающей обеспечение равноправного и взаимовыгодного сотрудничества всех заинтересованных сторон в информационной сфере;

9. Задачи государственных органов в рамках деятельности по обеспечению информационной безопасности?
обеспечение защиты прав и законных интересов граждан и организаций в информационной сфере;
оценка состояния информационной безопасности, прогнозирование и обнаружение информационных угроз, определение приоритетных направлений их предотвращения и ликвидации последствий их проявления;

планирование, осуществление и оценка эффективности комплекса мер по обеспечению информационной безопасности;
укрепление вертикали управления и централизация сил обеспечения информационной безопасности на федеральном, межрегиональном, региональном, муниципальном уровнях, а также на уровне объектов информатизации, операторов информационных систем и сетей связи;
повышение эффективности взаимодействия государственных органов, органов местного самоуправления, организаций и граждан при решении задач по обеспечению информационной безопасности;

10. Свойства информации:
конфиденциальность
целостность
доступность
непротиворечивость
доказуемость
все перечисленное

12. Информация, составляющая государственную тайну не может иметь гриф…
для служебного пользования
секретно
совершенно секретно
особой важности

13. В соответствии с нормами российского законодательства защита информации представляет собой принятие правовых, организационных и технических мер, направленных на …
обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации
соблюдение норм международного права в сфере информационной безопасности
выявление нарушителей и привлечение их к ответственности
соблюдение конфиденциальности информации ограниченного доступа
разработку методов и усовершенствование средств информационной безопасности

14. Система защиты государственных секретов
основывается на Уголовном Кодексе РФ
регулируется секретными нормативными документами
определена Законом РФ "О государственной тайне"
все перечисленное

15. Действие Закона "О государственной тайне" распространяется
на всех граждан и должностных лиц РФ
только на должностных лиц
на граждан, которые взяли на себя обязательство выполнять требования законодательства о государственной тайне
на всех граждан и должностных лиц, если им предоставили для работы закрытые сведения

16. К государственной тайне относится...
сведения в военной области
сведения о внешнеполитической и внешнеэкономической деятельности государства
сведения в области экономики, науки и техники
сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности
все перечисленное

17. Документы, содержащие государственную тайну снабжаются грифом
"секретно"
"совершенно секретно"
"особой важности"
все перечисленное

18. Гриф "ДСП" используется
для секретных документов
для документов, содержащих коммерческую тайну
как промежуточный для несекретных документов
в учебных целях

19. Порядок засекречивания состоит в установлении следующих принципов:
целесообразности и объективности
необходимости и обязательности
законности, обоснованности и своевременности
всех перечисленных

20. Предельный срок пересмотра ранее установленных грифов секретности составляет

5 лет
1 год
10 лет
15 лет
30 лет

21. Срок засекречивания сведений, составляющих государственную тайну
составляет 10 лет
ограничен 30 годами

22. Информация, составляющая государственную тайну не может иметь гриф…
«для служебного пользования»
«секретно»
«совершенно секретно»
«особой важности»

23. К государственной тайне относятся сведения о:
о запасах платины, металлов платиновой группы, природных алмазов в Государственном фонде драгоценных металлов и драгоценных камней Российской Федерации
о размерах золотого запаса и государственных валютных резервах Российской Федерации
о состоянии здоровья высших должностных лиц Российской Федерации

24. К государственной тайне относятся сведения о:
о финансовой политике в отношении иностранных государств
о чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, и их последствиях, а также о стихийных бедствиях, их официальных прогнозах и последствиях
о фактах нарушения законности органами государственной власти и их должностными лицами

25. Срок засекречивания сведений, составляющих государственную тайну, не должен превышать … лет.
30
25
15
10
50

26. Перечни сведений, подлежащих засекречиванию, подлежат пересмотру не реже, чем раз в … лет
5
7
10
15
30

27. Информация это –
сведения, поступающие от СМИ
только документированные сведения о лицах, предметах, фактах, событиях
сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления
только сведения, содержащиеся в электронных базах данных

28. Степени секретности информации
особой важности
совершенно секретно
секретно
для служебного пользования
не секретно

Примерный перечень вопросов к зачету:
1. Классификация угроз информационной безопасности автоматизированных систем по базовым признакам.
2. Угроза нарушения конфиденциальности. Особенности и примеры реализации угрозы.
3. Угроза нарушения целостности данных. Особенности и примеры реализации угрозы.
4. Угроза отказа служб (угроза отказа в доступе). Особенности и примеры реализации угрозы.
5. Понятие политики безопасности информационных систем. Назначение политики безопасности.
6. Основные типы политики безопасности доступа к данным. Дискреционные и мандатные политики.
7. Законодательный уровень обеспечения информационной безопасности. Основные законодательные акты РФ в области защиты информации.
8. Функции и назначение стандартов информационной безопасности. Примеры стандартов, их роль при проектировании и разработке информационных систем.
9. Критерии оценки безопасности компьютерных систем («Оранжевая книга»). Структура требований

безопасности. Классы защищенности.
10. Единые критерии безопасности информационных технологий. Понятие профиля защиты. Структура профиля защиты.
11. Единые критерии безопасности информационных технологий. Проект защиты. Требования безопасности (функциональные требования и требования адекватности).
12. Идентификация пользователей.
13. Аутентификация пользователей.
14. Авторизация.
15. Средства идентификации и аутентификации пользователей.
16. Защита от НСД.
17. Требования к СВТ.
18. Аудит в информационных системах. Функции и назначение аудита, его роль в обеспечении информационной безопасности.
19. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.
20. Защита персональных данных.
21. Защита информации в ГИС.
22. Концепция информационной безопасности.
23. Распределенные информационные системы. Удаленные атаки на информационную систему.
24. Каналы передачи данных. Утечка информации. Атаки на каналы передачи данных.
25. Физические средства обеспечения информационной безопасности.
26. Программно-аппаратные защиты информационных ресурсов в Интернет. Межсетевые экраны, их функции и назначения.
27. DLP-системы.

Задания:
Выполнить классификацию объекта информатизации.

1. Дано: В организации с частной формой собственности в качестве средств идентификации внедрена система, работающая на основе распознавания человека по отпечатку пальца или сетчатке глаза. Информация для распознавания хранится на сервере, работающем на платформе с сертифицированной ФСТЭК ОС Astra Linux Special Edition. Все системное и прикладное программное обеспечение выполнено в защищенном исполнении и проверено на отсутствие недекларированных возможностей.
В базе данных сотрудников обрабатывается менее 10000 субъектов ПДн. Выполнить классификацию ИСПДн сотрудников организации, хранящейся на сервере и используемой для проверки их личности.

2. Дано: В частной поликлинике обработка персональных данных пациентов. Обрабатывается менее 20000 записей о субъектах ПДн. Выполнить классификацию ИСПДн пациентов поликлиники при условии, что актуальны НДВ в прикладном программном обеспечении. В системном программном обеспечении угрозы не актуальны.

3. Дано: В районной управе ведется автоматизированная обработка информации о планируемой и проведенной работе по благоустройству территории. Определить класс защищенности информационной системы при условии, что невозможность работы с ней приведет к увеличению времени получения и обработки информации, снизит эффективность работы соответствующего подразделения.

4. Дано: В государственной организации на одном из компьютеров ведется обработка секретных сведений. За компьютером, кроме администратора, работают пользователи user1 и user2. При этом они обрабатывают одну и ту же информацию, имеют одинаковый доступ к файлам друг друга. Определить класс автоматизированной системы.

5. Дано: В библиотеке ведется учет посетителей на сервере с сертифицированной ФСТЭК ОС Astra Linux Special Edition. Для регистрации в библиотеке указываются паспортные данные – ФИО, адрес, номер телефона, учитывается выбор изданий. Обрабатывается менее 30000 записей о субъектах ПДн. Выполнить классификацию ИСПДн при условии, что НДВ в системном и прикладном программном обеспечении не актуальны.

6. Дано: В государственной организации проводятся исследования в области повышения эффективности изготовления и прочности строительных материалов. Материалы исследований засекречены. На компьютере, где хранится секретная информация с итогами исследования, работают два пользователя. Они проводят опыты с разными строительными материалами и не имеют доступ к файлам друг друга. Определите класс автоматизированной системы.

7. Дано: В земельном фонде автоматизированная система ведет учет участков, находящихся в государственной и муниципальной собственности в масштабах одного региона.
Обработка персональных данных в информационной системе не ведется.
Нарушение достоверности обрабатываемой информации может повлечь умеренные негативные последствия для экономики региона.

8. Дано: В частной торговой организации ведется учет покупателей с целью предоставления им бонусных скидок при последующей покупке товаров. В информационной системе ведется учет фамилии, имени, отчества, номера телефона и номера водительского удостоверения клиента.

В базе данных клиентов организации на момент классификации указано менее 3 тысяч человек. Потенциальный рост базы клиентов – не более 50 тысяч.
Обработка ведется на АРМ, где установлено лицензионное программное обеспечение.
Выполнить классификацию при условии, что:
1) НДВ в прикладном и системном ПО не актуальны.

5.2. Темы письменных работ

1) Абсолютно стойкий шифр

2) Американский стандарт криптозащиты

3) Криптографические средства идентификации пользователя

4) Аппаратно-программные комплексы защиты от НСД. Системы доверенной загрузки

5) Современные технологии защиты информации

6) Атаки на криптосистемы

7) Идентификация. Аутентификация. Управление доступом

8) Атаки на протоколы электронной подписи

9) Безопасность электронной почты

10) Блочные криптосистемы. Принципы построения

11) Вероятностное шифрование

12) Генераторы псевдослучайных последовательностей в задачах защиты информации

13) Государственная политика в сфере информатизации

14) Доктрина информационной безопасности РФ

15) Загрузочно-файловые вирусы

16) Задачи, решаемые криптографическими методами

17) Защита информации от случайных деструктивных воздействий

18) Защита информации от несанкционированного копирования

19) Защита ПО от статического и динамического исследования

20) Защита информации от несанкционированного доступа

21) Информационная безопасность личности, общества, государства

22) Квантовая криптография

23) Классификация криптоалгоритмов

24) Компьютерная преступность и компьютерная безопасность

25) Компьютерные вирус, их свойства и классификация. Антивирусы

26) Технологии зашиты видовой информации от утечки

27) Криптоанализ поточных шифров

28) Криптографические протоколы. Протокол выработки общего секретного ключа

29) Криптопроцессоры

30) Методы защиты от макровирусов

31) Методы сканирования уязвимостей

32) Механизмы функционирования пермутирующих, полиморфных и метаморфных вирусов. Защита от них

33) Неотвергаемая электронная подпись

34) Несимметричные протоколы аутентификации

35) Организационные методы защиты информации

36) Организация парольных систем

37) Технические методы защиты информации

38) Правовые акты в информационной сфере

39) Программные закладки и сетевые черви

40) Аттестация объектов информатизации

41) Пути проникновения вирусов в компьютер и механизм распределения вирусных программ

42) Контроль за обеспечением безопасной эксплуатации объектов информатизации

43) Российский стандарт криптозащиты. ГОСТ 28147-89

44) Сетевые вирусы

45) Симметричные криптосистемы

46) Синхронные и самосинхронизирующиеся поточные криптоалгоритмы

47) Система информационной безопасности человека

48) Системы обнаружения вторжений

49) Соотношение и взаимосвязь экономической и информационной безопасности личности

50) Сравнительный анализ стандартов информационной безопасности

51) Стеганографические методы защиты информации

52) Стелс-вирусы

53) Асимметричные криптосистемы

54) Технология Firewall

55) Технология цифровых водяных знаков

56) Троянские кони

57) Хакеры

58) Электронная цифровая подпись

59) Эффективность политик информационной безопасности

60) Классификация возможных каналов утечки информации

61) Технологии защиты акустической информации от утечки

62) Классификация методов зашиты информации от программно-математических воздействий

63) Деятельность администратора безопасности по предотвращению программно-математических воздействий

64) Технология разработки компьютерной системы защиты информации

5.3. Фонд оценочных средств

Вопрос 1:
Кто является основным ответственным за определение уровня классификации информации?
Варианты ответа:
а) Руководитель среднего звена
б) Высшее руководство
в) Владелец
г) Пользователь
Вопрос 2:
Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?
Варианты ответа:
а) Сотрудники
б) Хакеры
в) Атакующие
г) Контрагенты (лица, работающие по договору)
Вопрос 3:
Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?
Варианты ответа:
а) Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования
б) Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации
в) Улучшить контроль за безопасностью этой информации
г) Снизить уровень классификации этой информации
Вопрос 4:
Что самое главное должно продумать руководство при классификации данных?
Варианты ответа:
а) Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным
б) Необходимый уровень доступности, целостности и конфиденциальности
в) Оценить уровень риска и отменить контрмеры
г) Управление доступом, которое должно защищать данные
Вопрос 5:
Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?
Варианты ответа:
а) Владельцы данных
б) Пользователи
в) Администраторы
г) Руководство
Вопрос 6:
Что такое процедура?
Варианты ответа:
а) Правила использования программного и аппаратного обеспечения в компании
б) Пошаговая инструкция по выполнению задачи
в) Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах
г) Обязательные действия
Вопрос 7:
Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?
Варианты ответа:
а) Поддержка высшего руководства
б) Эффективные защитные меры и методы их внедрения
в) Актуальные и адекватные политики и процедуры безопасности
г) Проведение тренингов по безопасности для всех сотрудников
Вопрос 8:
Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?
Варианты ответа:
а) Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски
б) Когда риски не могут быть приняты во внимание по политическим соображениям
в) Когда необходимые защитные меры слишком сложны
г) Когда стоимость контрмер превышает ценность актива и потенциальные потери
Вопрос 9:
Что такое политики безопасности?
Варианты ответа:

а) Пошаговые инструкции по выполнению задач безопасности
б) Общие руководящие требования по достижению определенного уровня безопасности
в) Широкие, высокоуровневые заявления руководства
г) Детализированные документы по обработке инцидентов безопасности
Вопрос 10:
Какая из приведенных техник является самой важной при выборе конкретных защитных мер?
Варианты ответа:
а) Анализ рисков
б) Анализ затрат / выгоды
в) Результаты ALE
г) Выявление уязвимостей и угроз, являющихся причиной риска
Вопрос 11:
Что лучше всего описывает цель расчета ALE?
Варианты ответа:
а) Количественно оценить уровень безопасности среды
б) Оценить возможные потери для каждой контрмеры
в) Количественно оценить затраты / выгоды
г) Оценить потенциальные потери от угрозы в год
Вопрос 12:
Тактическое планирование – это:
Варианты ответа:
а) Среднесрочное планирование
б) Долгосрочное планирование
в) Ежедневное планирование
г) Планирование на 6 месяцев
Вопрос 13:
Что является определением воздействия (exposure) на безопасность?
Варианты ответа:
а) Нечто, приводящее к ущербу от угрозы
б) Любая потенциальная опасность для информации или систем
в) Любой недостаток или отсутствие информационной безопасности
г) Потенциальные потери от угрозы
Вопрос 14:
Эффективная программа безопасности требует сбалансированного применения:
Варианты ответа:
а) Технических и нетехнических методов
б) Контрмер и защитных механизмов
в) Физической безопасности и технических средств защиты
г) Процедур безопасности и шифрования
Вопрос 15:
Функциональность безопасности определяет ожидаемую работу механизмов безопасности, а гарантии определяют:
Варианты ответа:
а) Внедрение управления механизмами безопасности
б) Классификацию данных после внедрения механизмов безопасности
в) Уровень доверия, обеспечиваемый механизмом безопасности
г) Соотношение затрат / выгод

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	Шаньгин В. Ф.	Информационная безопасность компьютерных систем и сетей	Москва: Форум, 2021, URL: https://ibooks.ru/reading.php?short=1&productid=361273
Л1.2	Медведев В. А.	Информационная безопасность. Введение в специальность + еПриложение:Тесты: Учебник	Москва: КноРус, 2021, URL: https://book.ru/book/936335

	Авторы, составители	Заглавие	Издательство, год
Л1.3	Бабаш А. В., Баранова Е. К., Мельников Ю. Н.	Информационная безопасность. Лабораторный практикум + еПриложение: Учебное пособие	Москва: КноРус, 2021, URL: https://book.ru/book/936566
Л1.4	Мельников В. П., под ред., Куприянов А. И.	Информационная безопасность: Учебник	Москва: КноРус, 2021, URL: https://book.ru/book/939292
Л1.5	Мельников В. П., под ред., Куприянов А. И.	Информационная безопасность: Учебник	Москва: КноРус, 2020, URL: https://book.ru/book/932059
Л1.6	Мельников В. П., Куприянов А. И., Васильева Т. Ю.	Информационная безопасность: Учебник	Москва: КноРус, 2020, URL: https://book.ru/book/932908
Л1.7	Мельников В. П., Куприянов А. И., Васильева Т. Ю.	Информационная безопасность: Учебник	Москва: КноРус, 2022, URL: https://book.ru/book/941809
Л1.8	Озерский С.В., Попов И.В.	Информационная безопасность: Учебное пособие	Самара: Самарский юридический институт ФСИН России, 2019, URL: http://znanium.com/catalog/document?id=358668
Л1.9	Клименко И.С.	Информационная безопасность и защита информации: модели и методы управления: Монография	Москва: ООО "Научно-издательский центр ИНФРА-М", 2021, URL: http://znanium.com/catalog/document?id=360289
Л1.10	Шаньгин В.Ф.	Информационная безопасность компьютерных систем и сетей: Учебное пособие	Москва: Издательский Дом "ФОРУМ", 2021, URL: http://znanium.com/catalog/document?id=364622
Л1.11	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
Л1.12	Сычев Ю.Н.	Защита информации и информационная безопасность: Учебное пособие	Москва: ООО "Научно-издательский центр ИНФРА-М", 2021, URL: http://znanium.com/catalog/document?id=366835
Л1.13	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

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год
Л2.1	Козьминых С. И.	Информационная безопасность финансово-кредитных организаций в условиях цифровой трансформации экономики: Монография	Москва: КноРус, 2021, URL: https://book.ru/book/941548
Л2.2	Бабаш А. В., Баранова Е. К., Мельников Ю. Н.	Информационная безопасность. Практикум (+CD) (для бакалавров): Учебное пособие	Москва: КноРус, 2016, URL: https://book.ru/book/918700
Л2.3	Бабаш А. В., Баранова Е. К., Мельников Ю. Н.	Информационная безопасность. Лабораторный практикум (для бакалавров)+ Электронные приложения на сайте www.book.ru: Учебное пособие	Москва: КноРус, 2018, URL: https://book.ru/book/926191
Л2.4	Ищейнов В. Я.	Информационная безопасность и защита информации: словарь терминов и понятий: Словарь	Москва: Русайнс, 2019, URL: https://book.ru/book/932909
Л2.5	Мельников В. П., под ред., Куприянов А. И.	Информационная безопасность: Учебник	Москва: КноРус, 2018, URL: https://book.ru/book/924214

	Авторы, составители	Заглавие	Издательство, год
Л2.6	Ищейнов В. Я.	Информационная безопасность и защита информации: словарь терминов и понятий: Словарь	Москва: Русайнс, 2021, URL: https://book.ru/book/938255
Л2.7	Мельников В. П., Куприянов А. И., Васильева Т. Ю.	Информационная безопасность: Учебник	Москва: КноРус, 2018, URL: https://book.ru/book/929884
Л2.8	Ищейнов В. Я.	Информационная безопасность и защита информации: словарь терминов и понятий: Словарь	Москва: Русайнс, 2018, URL: https://book.ru/book/931784
Л2.9	Мельников В. П., Куприянов А. И., Васильева Т. Ю.	Информационная безопасность: Учебник	Москва: Русайнс, 2016, URL: https://book.ru/book/920736
Л2.10	Башлы П.Н., Бабаш А.В.	Информационная безопасность и защита информации: Учебник	Москва: Издательский Центр РИО□, 2013, URL: http://znanium.com/catalog/document?id=213488
Л2.11	Ковалев Д.В., Богданова Е.А.	Информационная безопасность: Учебное пособие	Ростов-на-Дону: Издательство Южного федерального университета (ЮФУ), 2016, URL: http://znanium.com/catalog/document?id=330789
Л2.12	Глинская Е.В., Чичварин Н.В.	Информационная безопасность конструкций ЭВМ и систем: Учебное пособие	Москва: ООО "Научно-издательский центр ИНФРА-М", 2021, URL: https://znanium.com/catalog/document?id=362430
Л2.13	Панфилова О.А., Крюкова Д.Ю.	Информационная безопасность и защита информации: Учебное пособие	Вологда: федеральное казенное образовательное учреждение высшего образования «Вологодский институт права и экономики Федеральной службы исполнения наказаний», 2018, URL: http://znanium.com/catalog/document?id=370184
Л2.14	Баранова Е.К., Бабаш А.В., Ларин Д.А.	Информационная безопасность. История специальных методов криптографической деятельности: Учебное пособие	Москва: Издательский Центр РИО□, 2022, URL: https://znanium.com/catalog/document?id=388319

6.2. Электронные учебные издания и электронные образовательные ресурсы

Э1	Совет Безопасности Российской Федерации . - Режим доступа: http://www.scrf.gov.ru/
Э2	Федеральная служба по техническому и экспортному контролю . - Режим доступа: https://fstec.ru/
Э3	Информационно-правовой портал ГАРАНТ.РУ . - Режим доступа: https://www.garant.ru/
Э4	Электронный фонд нормативно-технической и нормативно-правовой информации Консорциума «Кодекс» . - Режим доступа: https://docs.cntd.ru/
Э5	Национальный Открытый Университет "ИНТУИТ". - Режим доступа: https://intuit.ru/
Э6	Электронные ресурсы Академии ИМСИТ. - Режим доступа: http://eios.imsit.ru/
Э7	Электронная библиотечная система Znanium. - Режим доступа: http://znanium.com
Э8	Электронная библиотечная система Ibooks. - Режим доступа: http://www.ibooks.ru/
Э9	Электронная библиотечная система BOOK.ru. - Режим доступа: http://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	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
6.3.1.6	Notepad++. Тектовый редактор Notepad++. Программное обеспечение по лицензии GNU GPL
6.3.1.7	Kaspersky Endpoint Security Антивирусное ПО Kaspersky Endpoint Security для бизнеса Стандартный (350шт). Договор № ПР-00037842 от 4 декабря 2023 г. (ООО Прима АйТи)
6.3.1.8	Oracle VM VirtualBox VM VirtualBox — программный продукт виртуализации для операционных систем Программное обеспечение по лицензии GNU GPL

6.3.1.9	Adobe Reader DC Adobe Acrobat — пакет программ, предназначенный для создания и просмотра электронных публикаций в формате PDF Adobe Acrobat Reader DC and Runtime Software distribution license agreement for use on personal computers от 31.01.2017
6.3.1.1	MS Office Standart 2010 Офисный пакет Microsoft Office Microsoft Open License 48587685 от 02.06.2011
6.3.1.11	MS Visio Pro 2010 Интегрированная средда разработки Microsoft Visio профессиональный 2010 Подписка Microsoft Imagine Premium – Order №143659 от 12.07.2021
6.3.1.12	Windows 7 Pro Операционная система Microsoft Windows 7 Professional Microsoft Open License 48587685 от 02.06.2011
6.3.1.13	Консоль Kaspersky Security Center Консоль администрирования Kaspersky Security Center Договор № ПР-00035750 от 13 декабря 2022г. (ООО Прима АйТи)
6.3.1.14	Kaspersky Endpoint Security 11 Kaspersky Endpoint Security 11 для Windows Договор № ПР-00037842 от 4 декабря 2023 г. (ООО Прима АйТи)
6.3.1.15	Microsoft Windows 10 PRO x64 DSP OEM Операционная система Microsoft Windows 10 PRO Счет №93 от 21.05.2019, Акт передачи прав №31 от 05.06.2019.
6.3.1.16	10-Страйк Сканирование Сети Сканирование Сети - программа-сканер TCP-портов и IP-адресов Лицензионный сертификат от 01.01.2011
6.3.1.17	10-Страйк Инвентаризация Компьютеров Программа для учета ПК в сети предприятия Лицензионный сертификат от 01.01.2011
6.3.1.1	10-Strike File search pro Программа поиска файлов и документов в сети Лицензионный сертификат от 01.01.2011
6.3.1.19	Windows Server 2003 R2 Standart Операционная система Microsoft Windows Server 2003 R2 Microsoft Open License № 42060616 от 20.04.2007
6.3.1.20	Open SuSe Linux Опреационная система Open Source GNU/Linux Программное обеспечение по лицензии GNU GPL
6.3.1.21	Windows Server 2008 R2 Standart Операционная система Microsoft Windows Server 2008 Microsoft Open License № 46794243 от 19.04.2010
6.3.1.22	Traffic inspector Special Unlimited ОРГАНИЗАЦИЯ ДОСТУПА В ИНТЕРНЕТ. NAT, ПРОКСИ-СЕРВЕР, VPN, AD Лицензионный договор №649 от 23.09.2019
6.3.1.23	Эшэлон II “Кредо-диалог” Система зашиты Эшэлон II “Кредо-диалог” Акт № 123 от 01.11.2018, Сертификат от 24.08.2018
6.3.1.24	Система утпавления хранилищем документов “Кредо-диалог” Система утпавления хранилищем документов “Кредо-диалог” Акт № 123 от 01.11.2018, Сертификат от 24.08.2018
6.3.1.25	Astra Linux Операционная система семейства Linux. Версия "Орел" Программное обеспечение по лицензии GNU GPL
6.3.1.26	vGate Средство микросегментации и защиты жизненного цикла виртуальных машин Договор №КБ/04085/1/11 от 14.02.2022
6.3.1.27	Secren Net Studio Единая система управление продуктами для защиты Windows, Linux и платами доверенной загрузки Договор №КБ/04085/1/11 от 14.02.2022
6.3.1.28	Secren Net LSP Средство защиты информации от несанкционированного доступа для операционных систем семейства Linux Договор №КБ/04085/1/11 от 14.02.2022
6.3.2. Перечень профессиональных баз данных и информационных справочных систем	
6.3.2.1	Консультант Плюс http://www.consultant.ru
6.3.2.2	Global CIO Официальный портал ИТ-директоров http://www.globalcio.ru
6.3.2.3	ARIS BPM Community https://www.ariscommunity.com
6.3.2.4	ИСО Международная организация по стандартизации https://www.iso.org/ru/home.html
6.3.2.5	РОССТАНДАРТ Федеральное агентство по техническому регулированию и метрологии https://www.gost.ru/portal/gost/
6.3.2.6	Кодекс – Профессиональные справочные системы https://kodeks.ru

7. МТО (оборудование и технические средства обучения)

Ауд	Наименование	ПО	Оснащение
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	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

		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	
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
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 «Основы информационной безопасности» 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.

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ОБУЧАЮЩИМСЯ ПО ВЫПОЛНЕНИЮ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

Самостоятельная работа студентов в ходе семестра является важной составной частью учебного процесса и необходима для закрепления и углубления знаний, полученных в период сессии на лекциях, практических и интерактивных занятиях, а также для индивидуального изучения дисциплины «Основы информационной безопасности» в соответствии с программой и рекомендованной литературой.
Самостоятельная работа выполняется в виде подготовки домашнего задания или сообщения по отдельным вопросам, написание и защита научно-исследовательского проекта.
Контроль качества выполнения самостоятельной (домашней) работы может осуществляться с помощью устного опроса на лекциях или практических занятиях, обсуждения подготовленных научно-исследовательских проектов, проведения тестирования.
Устные формы контроля помогут оценить владение студентами жанрами научной речи (дискуссия, диспут, сообщение, доклад и др.), в которых раскрывается умение студентов передать нужную информацию, грамотно использовать языковые средства, а также ораторские приемы для контакта с аудиторией.
Письменные работы позволяют оценить владение источниками, научным стилем изложения, для которого характерны: логичность, точность терминологии, обобщенность и отвлеченность, насыщенность фактической информацией.