Троицкий Александр Витальевич

Федеральное государственное бюджетное образовательное учреждение высшего образования
«ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ ДВАЖДЫ ГЕРОЯ СОВЕТСКОГО СОЮЗА, ЛЕТЧИКА-КОСМОНАВТА А.А. ЛЕОНОВА»

Подписано цифровой подписью: Троицкий Александр Витальевич

«УТВЕРЖДАЮ»
И.о. проректора
_____ А.В. Троицкий
«___»_____2023 г.

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РАБОЧАЯ ПРОГРАММА
ДИСЦИПЛИНЫ (МОДУЛЯ)

Б.1.О.15.02 «ИНФОРМАЦИОННЫЕ ПРОЦЕССЫ И СИСТЕМЫ КАК ОБЪЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Направление подготовки: 10.03.01 Информационная безопасность

Профиль: Организация и технологии защиты информации

Уровень высшего образования: бакалавриат

Форма обучения: очная, очно-заочная

Королев
2023

Рабочая программа является составной частью основной профессиональной образовательной программы и проходит рецензирование со стороны работодателей в составе основной профессиональной образовательной программы. Рабочая программа актуализируется и корректируется ежегодно.

Автор: Пономаренко Г.В. Рабочая программа дисциплины: Информационные процессы и системы как объекты информационной безопасности. – Королев МО: «Технологический университет», 2023.

Рецензент: **Сухотерин А.И.**

Рабочая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по направлению подготовки бакалавров 10.03.01 «Информационная безопасность» и Учебного плана, утвержденного Ученым советом Университета. Протокол № 9 от 11.04.2023 года.

Рабочая программа рассмотрена и одобрена на заседании кафедры:

Заведующий кафедрой (ФИО, ученая степень, звание, подпись)	к.в.н., доцент Соляной В.Н.			
Год утверждения (переутверждения)	2023	2024	2025	2026
Номер и дата протокола заседания кафедры	№8 от 29.03.2023			

Рабочая программа согласована:

Руководитель ОПОП ВО Сухотерин А.И.

Рабочая программа рекомендована на заседании УМС:

Год утверждения (переутверждения)	2023	2024	2025	2026
Номер и дата протокола заседания УМС	№5 от 11.04.2023			

2

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ОПОП ВО

Целью изучения дисциплины является закрепление базовых положений по защите информации в процессе её передачи, обработки и хранения с применением существующих и перспективных информационных систем.

В процессе обучения студент приобретает и совершенствует следующие компетенции.

Дополнительные общепрофессиональные компетенции:

ДОПК-1. Способен проводить анализ функционального процесса объекта защиты и его информационных составляющих с целью выявления возможных источников информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба;

ДОПК-2. Способен формировать предложения по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы;

ДОПК-4. Способен проводить аудит защищенности объекта информатизации в соответствии с нормативными документами;

Основными **задачами** дисциплины являются:

1. Определение общей методологии защиты информации в информационных системах;
2. Освоение методических подходов в выборе способов и средств защиты информации;
3. Установление основных тенденций развития, направлений совершенствования информационных систем (ИС) и технологических операций, используемых при обработке данных;
4. Приобретение знаний по основам проектирования автоматизированных информационных систем (АИС), базирующимся на применении современных технических и программных средств с учётом требований безопасности;
5. Оценка степени защищённости информационных систем и алгоритмов их безопасного функционирования;
6. Приобретение навыков в решении задач сбора, хранения и обработки защищаемой информации, а также овладении приёмами работы с современными пакетами прикладных программ;

7. Определение основных угроз информационной безопасности информационных систем и факторов, влияющих на требуемый уровень их защищённости;

8. Определение путей совершенствования информационных систем с учётом требований по защите информации;

9. Определение методологических подходов к оценке эффективности информационных систем.

Показатель освоения компетенции отражают следующие индикаторы:

Необходимые знания:

- знает технологии обеспечения информационной безопасности, способы их организации и оптимизации
- знает технологии проектирования и построения информационных систем
- знает стратегии обеспечения информационной безопасности, способы их организации и оптимизации
- знает определения рисков информационной безопасности применительно к объекту информатизации с заданными характеристиками
- знает методы и подходы к реализации системы управления безопасностью автоматизированных информационных систем
- знает методы анализа процессов для определения актуальных угроз
- знает особенности работы решений по защите информации в информационных процессах и системах
- знает принципы обеспечения информационной безопасности объекта информатизаци
- знает основные категории требований к программным и программно-аппаратным средствам защиты информации
- знает требования по защите автоматизированных систем от НСД
- знает методы хранения, обработки и передачи и получения информации из открытых информационных систем
- знает подходы к построению подсистем фиксации и реагирования на инциденты информационной безопасности
- знает принципы разработки организационных и технических мер по сбору, анализу и мониторингу событий безопасности
- знает как проводится анализ журналов событий средств защиты информации
- знает основные этапы расследования компьютерных преступлений в соответствии с нормативными требованиями
- знает руководящие документы в области классификации современных информационных систем и средств вычислительной и техники
- знает основы нормативно-правовых актов в области защиты информации конфиденциального характера
- знает как формируется организационно-распорядительная и эксплуатационная документация по обеспечению безопасности информационных систем
- знает стандарты и критерии в области аудита ИБ

- знает требования законодательства по обеспечению безопасности персональных данных
- знает как составляются политики информационной безопасности в информационной системе персональных данных
- знает принципы организации процесса аудита
- знает теоретическую базу разработки политик безопасности
- знает теоретическую базу и средства для проведения мониторинга защищенности информационной системы
- знает принципы администрирования подсистем информационной безопасности
- знает порядок аттестации объектов информатизации
- знает порядок проведения сертификационных испытаний средств защиты информации

Необходимые умения:
- умеет обосновывать решения по обеспечению информационной безопасности объектов в профессиональной сфере деятельности
- умеет представлять процессы в формализованном виде на языках моделирования
- умеет делать выводы по результатам проведённого анализа, выявляя потенциальные угрозы ИБ
- умеет делать обоснованный выбор существующих средств защиты информации для нейтрализации определенного вида угроз
- владеет навыками выбора и применения современных аппаратных и программных средств технической защиты информации
- умеет анализировать эффективность применения мер по обеспечению ЗИ и разрабатывать предложения по совершенствованию структуры мер и повышению эффективности.
- умеет реагировать на инциденты информационной безопасности
- умеет сопоставлять основные структурно-функциональные характеристики информационных систем с требованиями руководящих документов
- умеет классифицировать информацию и автоматизированные системы, определять основные требования к ее защите
- умеет определять объекты аудита, критерии и область их действия
- умеет применять инструментальные средства мониторинга и аудита безопасности
- умеет составлять программу аудита ИБ
- умеет разрабатывать методики анализа рисков
- умеет собирать и анализировать свидетельства аудита
- умеет формализовать задачи анализа безопасности информационных систем

Трудовые действия:

- владеет навыками выявления и устранения угроз информационной безопасности
- владеет навыками реализации политики информационной безопасности
- владеет навыками применения современных программно-аппаратных средств моделирования информационных процессов и систем ЗИ
- владеет навыками оценки адекватности моделей и анализа результатов моделирования
- владеет навыками применения автоматизированных средств сбора и анализа информации, основанных на технологиях OSINT и data mining
- владеет навыками анализа надежности защиты информационных систем
- владеет навыками эффективного использования средств автоматического контроля и обнаружения возможных каналов утечки сведений, представляющих государственную, военную, служебную и коммерческую тайну
- владеет навыками классификации информационных систем и средств вычислительной техники по требованиям регуляторов ИБ
- владеет навыками сравнения и анализа существующих средств защиты информации
- владеет навыками нахождения наиболее подходящего решения применительно к заданным характеристикам информационной системы
- владеет навыками работы с нормативно-правовыми актами, навыками ориентации в них и поиска необходимой информации
- владеет навыками составления отчётов по результатам выполненного аудита
- владеет навыками проведения аудита ИБ со сбором данных
- владеет навыками по формулированию выводов и заключения по полученным результатам
- владеет навыками выбора и обоснования критериев оценки защищенности открытых информационных систем

2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Информационные процессы и системы как объекты информационной безопасности» относится к базовой части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Математика», «Информатика», «Пакеты прикладных программ» и компетенциях: ОК-8, ОПК-2,4 и ПК-1.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения всех последующих дисциплин «Конфиденциальное делопроизводство и защищенный электронный документооборот», «Моделирова-

ние процессов и систем защиты информации», «Информационная безопасность автоматизированных систем», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

3. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины для студентов очной и очно-заочной формы составляет 4 зачетных единицы, 144 часов.

Таблица1

Виды занятий	**Всего часов**	**Семестр** 4	**Семестр** 3	**Семестр**	**Семестр …**
Общая трудоемкость	144	144			
Аудиторные занятия	64	64			
Лекции (Л)	32	32			
Практические занятия (ПЗ)	32	32			
Лабораторные работы (ЛР)	-	-			
Самостоятельная работа	60	60			
Другие виды контактной работы	20	20			
Практическая подготовка	Нет	-			
Курсовые работы (проекты)	-	-			
Расчетно-графические работы	-	-			
Контрольная работа, домашнее задание	+	+			
Текущий контроль знаний (7 - 8, 15 - 16 недели)- 2ч.	Т1; Т2	Т1; Т2			
Вид итогового контроля	Экзамен	Экзамен			
ОЧНО - ЗАОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Виды занятий	**Всего часов**	**Семестр 5**	**Семестр 6**		
Общая трудоемкость	144	72	**72**		
Аудиторные занятия	40	20	20		
Лекции (Л)	16	8	8		
Практические занятия (ПЗ)	24	12	12		
Лабораторные работы (ЛР)	-	-	-		
Самостоятельная работа	102	51	51		
Другие виды контактной работы	**20**	**10**	**10**		
Курсовые работы (проекты)	-	-	-		
Расчетно-графические работы	-	-	-		
Контрольная работа, домашнее задание	+	+	+		
Практическая подготовка	4	2	2		
Вид итогового контроля	Зачет, экзамен	Зачет	Экзамен		

Под другими видами контактной работы понимается: групповые и индивидуальные консультации, тестирование

4. Содержание дисциплины

4.1.Темы дисциплины и виды занятий

Таблица 2

Наименование тем	Лекции, час. Очное/очно-заочное	Практические занятия, час Очное/очно-заочное	Занятия в интерактивной форме, час Очное/очно-заочное	Код компетенций
Тема 1: Введение. Информационный ресурс. Информатизация общества. Классификация информационных систем. Операционная схема процедуры восприятия и измерение информации	3/2	3/2	1/1	ДОПК-1
Тема 2: Обнаружение и распознавание информации. Принципы построения и основы применения информационных систем	3/2	3/2	1/1	ДОПК-1
Тема 3: Автоматизированные	3/2	3/2	1/1	ДОПК-2

информационные технологии и их классификация. Структурная и функциональная организация информационных систем и технологий				
Тема 4: Стадии и этапы создания автоматизированных информационных систем и технологий. Особенности проектирования автоматизированных информационных технологий	3/2	3/3	1/1	ДОПК-2
Тема 5: Структура и содержание информационного обеспечения. Технология применения электронного документооборота	4/2	4/3	1/1	ДОПК-2
Тема 6: Информационные базы и банки данных. Базы знаний. Цели и задачи технологического обеспечения. Режимы обработки информации	4/2	4/3	1/0.5	ДОПК-1,2,4
Тема 7: Экспертные информационные системы. Проблемы безопасности информационных систем	4/2	4/3	2/0.5	ДОПК-2

Тема 8: Организационно-правовые аспекты обеспечения информационной безопасности информационных систем. Комплексный (системный) подход в обеспечении информационной безопасности информационных систем	4/2	4/3	1/1	ДОПК-4
Тема 9: Методы и средства обеспечения информационной безопасности информационных систем	4/2	4/3	3/1	ДОПК-4
Итого:	32/16	32/24	12/8	

4.2. Содержание тем дисциплины

Тема 1. Введение. Информационный ресурс. Информатизация общества. Классификация информационных систем. Операционная схема процедуры восприятия и измерение информации

Предмет и задачи курса. Значение и место курса в подготовке специалистов по защите информации. Научная и учебная взаимосвязь курса с другими дисциплинами.

Разделы и темы, их распределение по видам аудиторных занятий. Формы проведения практических занятий. Состав и методика самостоятельной работы студентов по изучению дисциплины. Формы проверки знаний.

Анализ нормативных источников, научной и учебной литературы.

Знания и умения студентов, которые должны быть получены в результате изучения курса.

Становление и развитие понятия "информационные процессы". Современные подходы к определению понятия «информатизация».

Две стороны задачи восприятия. Цель измерительного преобразования. Угловая и временная формы представления параметров передаваемой информации. Операционная схема процедуры восприятия. Первичное восприятие и измерение информации.

Тема 2. Обнаружение и распознавание информации. Принципы по-

строения и основы применения информационных систем

Задачи обнаружения и распознавания информации. Характеристика пространства признаков и его разбиение. Вероятностный подход при рассмотрении зависимости реализаций от состояний. Характерные случаи расположения условных распределений. Качество распознавания и его параметры.

Структура информационных ресурсов. Основные свойства информационных систем. Структурированность информационных систем. Принципы построения информационных систем. Многоуровневость и распределённость информационных систем. Особенности применения информационных систем в различных областях. Интегрированные информационные системы.

Тема 3. Автоматизированные информационные технологии и их классификация. Структурная и функциональная организация информационных систем и технологий

Определение автоматизированных информационных технологий (АИТ). Основные компоненты АИТ. Виды классификаций АИТ. Основные тенденции развития АИТ в современных условиях. Интегрированные информационные системы обработки данных и способы защиты информации. Многоуровневые и распределённые информационные системы организационного управления.

Система управления и её роль в процессе получения информации и её обработки с помощью заданных алгоритмов. Технологические процессы при обработке данных. Основные задачи автоматизированных информационных систем (АИС). Структура и составные элементы АИС и АИТ. Функции АИТ. Процедуры преобразования информации в АИС. Технология функционирования элементов АИТ

Тема 4. Стадии и этапы создания автоматизированных информационных систем и технологий. Особенности проектирования автоматизированных информационных технологий

Цель и задачи проектирования АИТ и АИС. Основополагающие принципы создания АИС. Принцип системности – важнейший принцип при создании, функционировании и развитии АИС. Стадии жизненного цикла АИС и АИТ. Модели жизненного цикла АИС и АИТ. Особенности разработки АИС и АИТ.

Особенности создания АИТ. Основные требования к АИТ с учётом информационной безопасности. Аппаратно-программные комплексы, используемые при создании АИТ. Классы пользователей АИТ.

Тема 5. Структура и содержание информационного обеспечения. Технология применения электронного документооборота

Определение информационного обеспечения. Организация информационного обеспечения. Классификаторы, коды и технология их применения. Выбор системы кодирования. Последовательность разработки позиционных и комбинированных систем кодирования.

Последовательность прохождения документов. Автоматизация движения информационных потоков. Система поиска. Механизм установления

паролей на вход в информационную систему и выбор способа шифрования данных.

Тема 6. Информационные базы и банки данных. Базы знаний. Цели и задачи технологического обеспечения. Режимы обработки информации

Технология информационных баз и банков данных. Требования, предъявляемые к информационным базам данных. Распределённая система информационных баз и банков данных. Этапы создания информационных баз и банков данных. Система управления базами данных (СУБД). Управленческие стандарты информационной безопасности.

Техническое обеспечение. Средства обработки информации. Распределённая система обработки информации. Условия разработки и выбора программного обеспечения. Классификация программного обеспечения. Диалоговый режим обработки информации. Сетевой режим обработки информации.

Тема 7. Экспертные информационные системы. Проблемы безопасности информационных систем

Определение экспертной системы. Технология применения экспертных систем. Разработка экспертных систем. Преимущества использования экспертных систем. Отличительные особенности экспертных систем. Области применения экспертных систем. Уязвимость экспертных систем.

Причины, способствующие уязвимости информационных систем. Источники, виды и анализ угроз. Мероприятия по предотвращению угроз безопасности информационных систем. Проблемы обеспечения безопасности информационных систем. Основные подходы в создании защищённых информационных систем.

Тема 8. Организационно-правовые аспекты обеспечения информационной безопасности информационных систем. Комплексный (системный) подход в обеспечении информационной безопасности информационных систем

Глобальные информационные сети и системы, их свойства. Правовые аспекты информационного обмена в глобальных сетях. Особенности отношений субъектов информационного обмена в сетях. Обеспечение совместимости в информационных сетях и системах. Протоколы совместимости. Роль стандартов информационной безопасности при создании информационных систем.

Основные стадии жизненного цикла системы защиты информации. Общая методология в выборе средств и способов защиты информации в информационных системах. Модель построения системы защиты информации. Комплексный (системный) подход в обеспечении информационной безопасности информационных систем.

Тема 9. Методы и средства обеспечения информационной безопасности информационных систем

Методы и средства защиты информации в информационных системах. Два подхода к проблеме обеспечения информационной безопасности

информационных систем. Пути решения проблем защиты информации в информационных системах. Задачи управления средствами информационной безопасности. Политики безопасности. Протоколы безопасной передачи данных.

5. Перечень учебно-методического обеспечения для самостоятельной работы по дисциплине

«Методические указания для самостоятельной работы обучающихся по освоению дисциплины» представлены в Приложении 2.

6. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

Структура фонда оценочных средств, для проведения промежуточной аттестации обучающихся по дисциплине «Информационные процессы, системы и их безопасность» приведена в Приложении 1.

7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Основная литература:

1.Чернышев, А. Б. Теория информационных процессов и систем : учебное пособие / А. Б. Чернышев, В. Ф. Антонов, Г. Б. Суюнова. — Ставрополь : СКФУ, 2015. — 169 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/155262 (дата обращения: 23.12.2022). — Режим доступа: для авториз. пользователей.

2.Овсянников, А. С. Теория информационных процессов и систем : учебник / А. С. Овсянников. — Самара : ПГУТИ, 2019. — 274 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/223301 (дата обращения: 23.12.2022). — Режим доступа: для авториз. пользователей.

Дополнительная литература:

3.Теория информационных процессов и систем : учебное пособие. — Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2016 — Часть 1 — 2016. — 67 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/180067 (дата обращения: 23.12.2022). — Режим доступа: для авториз. пользователей.

4.Теория информационных процессов и систем : учебное пособие. — Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2016 — Часть 2 — 2016. — 87 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/180064 (дата обращения: 23.12.2022). — Режим доступа: для авториз. пользователей.

8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

Интернет-ресурсы:

1. **http://eup.ru/catalog/all-all.asp –** научно-образовательный портал.
2. **http://informika.ru/** – образовательный портал.
3. **www.wikIsec.ru** - Энциклопедия информационной безопасности. – Публикации, статьи.
4. **www.biblioclub.ru** - Универсальная библиотека онлайн.
5. **www.rucont.ru** - ЭБС «Руконт».
6. **http://www.academy.it.ru/** - академия АЙТИ.
7. **http://www.minfin.ru** - Официальный сайт Министерства финансов Российской Федерации
8. **http://www.gov.ru/** - Официальный сервер органов государственной власти Российской Федерации.
9. **http://www.fsb.ru/** - Официальный сайт Федеральной Службы Безопасности
10. **http://www.fstec.ru/** - Официальный сайт Федеральной Службы по Техническому Экспортному контролю

9. Методические указания для обучающихся, по освоению дисциплины

Методические указания для обучающихся, по освоению дисциплины (модуля) приведены в Приложении 2 к настоящей рабочей программе.

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

- **Перечень программного обеспечения:** MSOffice, PowerPoint.
- **Информационные справочные системы:**

1. Электронные ресурсы образовательной среды Университета.
2. Рабочая программа и методическое обеспечение по дисциплине: «Информационные процессы и системы как объекты информационной безопасности»

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Лекционные занятия:

- аудитория, оснащенная презентационной техникой (проектор, экран);
- комплект электронных презентаций / слайдов на темы:

Практические занятия:

- компьютерный класс с проектором для интерактивного обучения и проведения лекций в форме слайд-презентаций, оборудованный современ-

ными лицензионными программно-техническими средствами: операционная система не ниже WindowsXP; офисные программы MSOffice 7;

- рабочее место преподавателя, оснащенное компьютером с доступом в Интернет;
- рабочие места студентов, оснащенные компьютерами с доступом в Интернет.

Приложение 1

Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю)

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

«ИНФОРМАЦИОННЫЕ ПРОЦЕССЫ И СИСТЕМЫ КАК ОБЪЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Направление подготовки: 10.03.01 «Информационная безопасность»

Профиль: Организация и технологии защиты информации

Уровень высшего образования: бакалавриат

Форма обучения: очная, очно-заочная

Королев
2023

1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

№ п/п	Индекс компетенции	Содержание компетенции	Раздел дисциплины, обеспечивающий формирование компетенции	В результате изучения раздела дисциплины, обеспечивающего формирование компетенции, обучающийся приобретает		
				Трудовые действия	Необходимые умения	Необходимые знания
1.	ДОПК-1	Способен проводить анализ функционального процесса объекта защиты и его информационных составляющих с целью выявления возможных источников информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба	Темы 1, 2,3, 4, 5,6, 7, 8, 9	- владеет навыками выявления и устранения угроз информационной безопасности - владеет навыками реализации политики информационной безопасности - владеет навыками применения современных программно-аппаратных средств моделирования информационных процессов и систем ЗИ - владеет навыками оценки адекватности моделей и анализа результатов моделирования - владеет навыками применения автоматизированных	- умеет обосновывать решения по обеспечению информационной безопасности объектов в профессиональной сфере деятельности - умеет представлять процессы в формализованном виде на языках моделирования - умеет делать выводы по результатам проведённого анализа, выявляя потенциальные угрозы ИБ - умеет делать обоснованный выбор существующих средств защиты информации для нейтрализации определенного вида угроз	- знает технологии обеспечения информационной безопасности, способы их организации и оптимизации - знает технологии проектирования и построения информационных систем - знает стратегии обеспечения информационной безопасности, способы их организации и оптимизации - знает определения рисков информационной безопасности применительно к объекту информатизации с заданными характеристиками - знает методы и подходы к реализации системы управления безопасностью автоматизированных информационных систем - знает методы анализа процессов для определения актуальных угроз - знает особенности работы ре-

				средств сбора и анализа информации, основанных на технологиях OSINT и data mining - владеет навыками анализа надежности защиты информационных систем - владеет навыками эффективного использования средств автоматического контроля и обнаружения возможных каналов утечки сведений, представляющих государственную, военную, служебную и коммерческую тайну	- владеет навыками выбора и применения современных аппаратных и программных средств технической защиты информации	шений по защите информации в информационных процессах и системах - знает принципы обеспечения информационной безопасности объекта информатизаци - знает основные категории требований к программным и программно-аппаратным средствам защиты информации - знает требования по защите автоматизированных систем от НСД - знает методы хранения, обработки и передачи и получения информации из открытых информационных систем
2.	ДОПК-2	Способен формировать предложения по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы;	Темы 1, 2,3, 4, 5,6, 7, 8, 9	- владеет навыками классификации информационных систем и средств вычислительной техники по требованиям регуляторов ИБ - владеет навы-	- умеет анализировать эффективность применения мер по обеспечению ЗИ и разрабатывать предложения по совершенствованию структуры мер и по-	- знает подходы к построению подсистем фиксации и реагирования на инциденты информационной безопасности - знает принципы разработки организационных и технических мер по сбору, анализу и мониторингу со-

				ками сравнения и анализа существующих средств защиты информации - владеет навыками нахождения наиболее подходящего решения применительно к заданным характеристикам информационной системы- - владеет навыками работы с нормативно-правовыми актами, навыками ориентации в них и поиска необходимой информации	вышению эффективности. - умеет реагировать на инциденты информационной безопасности - умеет сопоставлять основные структурно-функциональные характеристики информационных систем с требованиями руководящих документов - умеет классифицировать информацию и автоматизированные системы, определять основные требования к ее защите	бытий безопасности - знает как проводится анализ журналов событий средств защиты информации - знает основные этапы расследования компьютерных преступлений в соответствии с нормативными требованиями - знает руководящие документы в области классификации современных информационных систем и средств вычислительной и техники - знает основы нормативно-правовых актов в области защиты информации конфиденциального характера - знает как формируется организационно-распорядительная и эксплуатационная документация по обеспечению безопасности информационных систем
3.	ДОПК-4	Способен проводить аудит защищенности объекта информатизации в соответствии с нормативными документами	Темы 1, 2,3, 4, 5,6, 7, 8, 9	- владеет навыками составления отчётов по результатам выполнен-	- умеет определять объекты аудита, критерии и область их действия	- знает стандарты и критерии в области аудита ИБ - знает требования законодательства по

				ного аудита владеет навыками проведения аудита ИБ со сбором данных - владеет навыками по формулированию выводов и заключения по полученным результатам - владеет навыками выбора и обоснования критериев оценки защищенности открытых информационных систем	- умеет применять инструментальные средства мониторинга и аудита безопасности - умеет составлять программу аудита ИБ - умеет разрабатывать методики анализа рисков - умеет собирать и анализировать свидетельства аудита умеет формализовать задачи анализа безопасности информационных систем	обеспечению безопасности персональных данных - знает как составляются политики информационной безопасности в информационной системе персональных данных - знает принципы организации процесса аудита - знает теоретическую базу разработки политик безопасности - знает теоретическую базу и средства для проведения мониторинга защищенности информационной системы - знает принципы администрирования подсистем информационной безопасности - знает порядок аттестации объектов информатизации - знает порядок проведения сертификационных испытаний средств защиты информации

2.Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Код компетенции	*Инструмент, оценивающий сформированность компетенции*	*Этапы и показатель оценивания компетенции*	*Критерии оценивания компетенции на различных этапах формирования и шкалы оценивания*
ДОПК-1,2,4	*Доклад*	*А) полностью сформирована (компетенция освоена на высоком уровне) – 5 баллов* *Б) частично сформирована:* • ***компетенция освоена на продвинутом уровне – 4 балла;*** • ***компетенция освоена на базовом уровне – 3 балла;*** *В) не сформирована (компетенция не сформирована) – 2 и менее баллов*	*Например:* ***Проводится в письменной и/или устной форме.*** *Критерии оценки:* *1. Соответствие содержания доклада заявленной тематике (1 балл).* *2. Качество источников и их количество при подготовке работы (1 балл).* *3. Владение информацией и способность отвечать на вопросы аудитории (1 балл).* *4. Качество самой представленной работы (1 балл).* *5. Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл).* ***Максимальная сумма баллов - 5 баллов.***
ДОПК-1,2,4	*Выполнение контрольной работы*	*А) полностью сформирована (компетенция освоена на высоком уровне) – 5 баллов* *Б) частично сформирована:* • ***компетенция освоена на продвинутом уровне – 4 балла;*** • ***компетенция освоена на базовом уровне – 3 балла;*** *В) не сформирована (компетенция не сформирована) – 2 и менее баллов*	*При определении сформированности компетенций критериями оценивания выступают методические рекомендации, разработанные по дисциплине для данного вида*

3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Примерная тематика докладов в презентационной форме:

1. Виды атак на сетевые информационные системы и методы борьбы с ними.
2. Скорость передачи информации дискретных каналов с помехами.
3. Современные системы электронного документооборота и показатели их защищённости.
4. Информационная безопасность электронного бизнеса.

5. Оптимальные алгоритмы обработки конфиденциальной информации в сетевых информационных системах.

6. Методы оценки эффективности функционирования современных информационных систем.

7. Перспективные информационные системы, технологии управления и обеспечение их безопасности.

8. Методы разграничения доступа в информационных системах.

9. Интегрированные и корпоративные информационные системы, проблемы их защищённости.

10. Статистические критерии обнаружения и распознавания информации.

4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Формой контроля знаний по дисциплине «Информационные процессы и системы как объекты информационной безопасности» являются две текущие аттестации в виде тестов и итоговая аттестация в виде зачета.

Неделя текущего контроля	Вид оценочного средства	Код компетенций, оценивающий знания, умения, навыки	Содержание оценочного средства	Требования к выполнению	Срок сдачи (неделя семестра)	Критерии оценки по содержанию и качеству с указанием баллов
Проводится в сроки, установленные графиком образовательного процесса	тестирование	ДОПК-1,2,4	20-40 вопросов	***Компьютерное тестирование. Время, отведенное на процедуру – 30 минут***	***Результаты тестирования предоставляются в день проведения процедуры***	***Преподаватель указывает критерии оценки данного вида контроля. Например, критерии оценки определяются процентным соотношением. Неявка – 0. Неудовлетворительно – менее 50% правильных ответов Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%.***
Проводится в сроки, установленные графиком образовательного процесса	тестирование	ДОПК-1,2,4	20 вопросов	***Компьютерное тестирование. Время, отведенное на процедуру – 30 минут***	***Результаты тестирования предоставляются в день проведения процедуры***	***Преподаватель указывает критерии оценки данного вида контроля. Например, критерии оценки определяются процентным соотношением. Неявка – 0. Неудовлетворительно – менее 50% правильных ответов Удовлетворительно - от 51% правильных***

						ответов. Хорошо - от 70%. Отлично – от 90%.
Проводится в сроки, установленные графиком образовательного процесса	Зачет /экзамен	ДОПК-1,2,4	2 теоретических вопроса + практическое задание	Зачет проводится в письменной форме, путем ответа на вопросы. Время, отведенное на процедуру – 15 /30 минут.	Результаты предоставляются в день проведения зачета	Критерии оценки: «**Отлично**»: • знание основных понятий предмета; • умение использовать и применять полученные знания на практике; • работа на практических занятиях; • знание основных научных теорий, изучаемых предметов; • ответ на вопросы билета. «**Хорошо**»: • знание основных понятий предмета; • умение использовать и применять полученные знания на практике; • работа на практических занятиях; • знание основных научных теорий, изучаемых предметов; • ответы на вопросы билета • неправильно решено практическое задание «У**довлетворительно**»: • демонстрирует частичные знания по темам дисциплин; • незнание неумение использовать и

						применять полученные знания на практике; • не работал на практических занятиях; «**Неудовлетвори-тельно**»: • демонстрирует частичные знания по темам дисциплин; • незнание основных понятий предмета; • неумение использовать и применять полученные знания на практике; • не работал на практических занятиях; • не отвечает на вопросы.

Примерное содержание тестов для текущей аттестации:

4.1. Типовые вопросы, выносимые на тестирование

Тесты используются в режиме промежуточного контроля. По форме заданий выбраны открытые тесты.

1. Перечислите возможные каналы утечки информации в офисном помещении?

2. Изобразите модель системы защиты информации?

3. Поясните организацию обмена данными в информационных системах?

4. Дайте определение системы защиты информации от несанкционированного доступа?

5. Что подразумевается под безопасностью информационной системы (ИС)?

6. Изобразить структуру информационных ресурсов?

7. Перечислить основные виды угроз безопасности?

8. Перечислить наиболее распространенные пути НСД к информации?

9. Назвать задачи, решаемые при проектировании автоматизированных информационных технологий?

10. Перечислить организационные меры по защите информации?

11. Дайте определение идентификации и аутентификации?

12. Назвать особенности парольных систем аутентификации и угрозы их безопасности?

13. Перечислить рекомендации по практической реализации парольных систем?

14. Какие методы хранения паролей существуют?

15. Назвать методы разграничения доступа и их отличительные особенности?

16. Пояснить схему симметричного криптошифрования?

17. Пояснить схему асимметричного криптошифрования?

18. Пояснить назначение механизма регистрации и аудита?

19. Куда и как помещаются протоколируемые данные?

20. Изобразить схему отношения субъектов информационного обмена в сети Internet?

21. В чем сущность главной задачи, решаемой при создании сетевых ИС?

22. Что представляет собой модель OSI?

23. Что такое стек коммуникационных протоколов и межуровневый интерфейс?

24. Что используют в компьютерных сетях для подслушивания?

25. В чем сущность подмены доверенного субъекта?

26. С какой целью осуществляется посредничество в обмене информационными ключами?

27. Чем характеризуется отказ в обслуживании?

28. Дайте характеристику парольным атакам?

29. Что представляет собой сетевая разведка?

30. Какие подходы к проблеме обеспечения безопасности ИС и сетей существуют?

31. Перечислить группы административно-организационных мер?

32. Какие механизмы безопасности используют современные ИС?

33. Назовите области ИБ, на которые должны опираться создатели электронного бизнеса?

34. Перечислите основные методы и средства защиты информации в рамках общей системы ИБ?

35. По каким признакам классифицируются компьютерные вирусы?

36. Дайте характеристику сетевым компьютерным вирусам?

37. Что такое «Троянские программы» и «Логические бомбы»?

38. Перечислить основные каналы распространения компьютерных вирусов?

39. Назовите основные методы защиты от компьютерных вирусов?

40. В чем сущность концепции глобального управления безопасностью?

41. Назвать структурные элементы системы управления средствами безопасности?

42. Дайте краткую характеристику отечественным стандартам ИБ?

43. Какие стандарты ИБ для беспроводных сетей существуют?

44. Дайте общую характеристику стандарту ISO/IEC 15408-1999?

45. Дайте общую характеристику стандарту ISO/IEC 15408-1999?

46. Перечислите международные стандарты ИБ?

4.2. Типовые вопросы, выносимые на зачет

1. Понятие "информационный процесс". Восприятие информации.
2. Операционная схема процедуры восприятия информации.
3. Две стороны задачи восприятия. Цель измерительного преобразования.
4. Угловая и временная формы представления параметров передаваемой информации.
5. Первичное восприятие и измерение информации.
6. Задачи обнаружения и распознавания информации.
7. Характеристика пространства признаков и его разбиение.
8. Качество распознавания и его параметры.
9. Свойства информационных систем. Структурированность информационных систем.
10. Принципы построения защищённых информационных систем.
11. Интегрированные информационные системы и их защищённость.
12. Основные тенденции развития АИТ в современных условиях.
13. Интегрированные информационные системы обработки данных и способы защиты информации.
14. Многоуровневые и распределённые информационные системы организационного управления.
15. Структура и составные элементы АИС и АИТ. Функции АИТ.
16. Процедуры преобразования информации в АИС. Технология функционирования элементов АИТ.
17. Определение информационного обеспечения. Организация информационного обеспечения.
18. Выбор системы кодирования. Последовательность разработки позиционных и комбинированных систем кодирования.
19. Автоматизация движения информационных потоков. Система поиска.
20. Механизм установления паролей на вход в информационную систему и выбор способа шифрования данных.
21. Требования, предъявляемые к информационным базам данных.
22. Распределённая система информационных баз и банков данных.
23. Система управления базами данных (СУБД). Управленческие стандарты информационной безопасности.
24. Техническое обеспечение. Средства обработки информации.
25. Распределённая система обработки информации.

26. Диалоговый режим обработки информации.

27. Сетевой режим обработки информации.

28. Причины, способствующие уязвимости информационных систем. Источники, виды и анализ угроз.

29. Мероприятия по предотвращению угроз безопасности информационных систем.

30. Проблемы обеспечения безопасности информационных систем. Основные подходы в создании защищённых информационных систем.

31. Глобальные информационные сети и системы, их свойства.

32. Правовые аспекты информационного обмена в глобальных сетях.

33. Обеспечение совместимости в информационных сетях и системах. Протоколы совместимости.

34. Роль стандартов информационной безопасности при создании информационных систем.

35. Основные стадии жизненного цикла системы защиты информации.

36. Общая методология в выборе средств и способов защиты информации в информационных системах.

37. Модель построения системы защиты информации.

38. Комплексный (системный) подход в обеспечении информационной безопасности информационных систем.

39. Методы и средства защиты информации в информационных системах.

40. Два подхода к проблеме обеспечения информационной безопасности информационных систем.

41. Пути решения проблем защиты информации в информационных системах.

42. Задачи управления средствами информационной безопасности. Политики безопасности.

43. Протоколы безопасной передачи данных.

44. Свойства и параметры сложных информационных систем.

45. Механизм установления паролей на вход в информационную систему и выбор способа шифрования данных.

**Итоговое начисление баллов по дисциплине осуществляется в соответствии с разработанной и внедренной балльно-рейтинговой системой контроля и оценивания уровня знаний и внеучебной созидательной активности обучающихся.*

Приложение 2

Методические указания для обучающихся по освоению дисциплины (модуля)

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

«ИНФОРМАЦИОННЫЕ ПРОЦЕССЫ И СИСТЕМЫ КАК ОБЪЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Направление подготовки: 10.03.01 «Информационная безопасность»

Профиль: Организация и технологии защиты информации

Уровень высшего образования: бакалавриат

Форма обучения: очная, очно-заочная

Королев
2023

1. Общие положения

Целью изучения дисциплины является:

1. Формирование у студентов специализированной базы знаний по фундаментальным проблемам информационной безопасности в условиях становления современного информационного общества.
2. закрепление базовых положений по защите информации в процессе её передачи, обработки и хранения с применением существующих и перспективных информационных систем.
3. Получение первичных навыков в применении защищённых технологий при обеспечении информационной безопасности различных объектов.

Задачи дисциплины:

- ознакомление студентов с информационными процессами на предприятии с точки зрения информационной безопасности;
- формирование у студентов способности самостоятельно проводить классификацию автоматизированных систем и средств защиты информации по требованиям безопасности;
- формирование студентами предложений по совершенствованию, модернизации, унификации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами.

2. Указания по проведению практических занятий

Тема 1: Введение. Информационный ресурс. Информатизация общества. Классификация информационных систем. Операционная схема процедуры восприятия и измерение информации

Практическое занятие 1.

Вид практического занятия**:** ***подготовка доклада.***

Образовательные технологии: ***групповая дискуссия.***

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Ознакомиться с основными понятиями.

Основные положения темы занятия:

1. Становление и развитие понятия "информационные процессы".
2. Современные подходы к определению понятия «информатизация».

Вопросы для обсуждения:

Основной доклад (реферат) по теме занятия.

1. Две стороны задачи восприятия.

2. Цель измерительного преобразования.

3. Угловая и временная формы представления параметров передаваемой информации.

4. Операционная схема процедуры восприятия.

5. Первичное восприятие и измерение информации.

продолжительность занятия – 3/2

Тема 2: Обнаружение и распознавание информации. Принципы построения и основы применения информационных систем

Практическое занятие 2.

Вид практического занятия**:** ***подготовка доклада.***

Образовательные технологии: ***групповая дискуссия.***

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Ознакомиться с принципами построения информационных систем

Основные положения темы занятия:

1. Основные свойства информационных систем.

2. Принципы построения информационных систем.

Вопросы для обсуждения:

Основной доклад (реферат) по теме занятия.

1. Задачи обнаружения и распознавания информации

2. Многоуровневость и распределённость информационных систем.

3. Особенности применения информационных систем в различных областях

продолжительность занятия – 3/2

Тема 3: Автоматизированные информационные технологии и их классификация. Структурная и функциональная организация информационных систем и технологий

Практическое занятие 3.

Вид практического занятия**:** ***подготовка доклада.***

Образовательные технологии: ***групповая дискуссия.***

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Ознакомиться с организацией информационных систем и технологий.

Основные положения темы занятия:

1. Многоуровневые и распределённые информационные системы организационного управления.

2. Система управления и её роль в процессе получения информации и её обработки с помощью заданных алгоритмов

Вопросы для обсуждения:

Основной доклад (реферат) по теме занятия.

1. Основные компоненты АИТ. Виды классификаций АИТ.
2. Основные задачи автоматизированных информационных систем (АИС)

продолжительность занятия – 3/2

Тема 4: Стадии и этапы создания автоматизированных информационных систем и технологий. Особенности проектирования автоматизированных информационных технологий

Практическое занятие 4.

Вид практического занятия**:** ***подготовка доклада.***

Образовательные технологии: ***групповая дискуссия.***

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить базовые знания о проектировании и построении автоматизированных информационных систем.

Основные положения темы занятия:

1. Цель и задачи проектирования АИТ и АИС
2. Особенности создания АИТ

Вопросы для обсуждения:

Основной доклад (реферат) по теме занятия.

1. Стадии жизненного цикла АИС и АИТ.
2. Особенности разработки АИС и АИТ.
3. Классы пользователей АИТ.

продолжительность занятия – 3/2

Тема 5: Структура и содержание информационного обеспечения. Технология применения электронного документооборота

Практическое занятие 5.

Вид практического занятия**:** ***подготовка доклада.***

Образовательные технологии: ***групповая дискуссия.***

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить представление об информационном обеспечении и электронном документообороте.

Основные положения темы занятия:

1. Ознакомиться с организацией информационного обеспечения
2. Ознакомиться с автоматизацией движения информационных потоков

Вопросы для обсуждения:

Основной доклад (реферат) по теме занятия.

1. Последовательность разработки позиционных и комбинированных систем кодирования.
2. Механизм установления паролей на вход в информационную систему и выбор способа шифрования данных

продолжительность занятия – 3/2

Тема 6: Информационные базы и банки данных. Базы знаний. Цели и задачи технологического обеспечения. Режимы обработки информации
Практическое занятие 6.

Вид практического занятия**:** ***подготовка доклада.***
Образовательные технологии: ***групповая дискуссия.***

Вид практического занятия**:** *смешанная форма практического занятия.*
Тема и содержание практического занятия:
Цель работы: Получить практические навыки в предоставлении технологического обеспечения.

Основные положения темы занятия:

1. Технология информационных баз и банков данных.
2. Средства обработки информации.

Вопросы для обсуждения:

Основной доклад (реферат) по теме занятия.
1. Требования, предъявляемые к информационным базам данных.
2. Система управления базами данных (СУБД).
3. Условия разработки и выбора программного обеспечения

продолжительность занятия – 3/2

Тема 7: Экспертные информационные системы. Проблемы безопасности информационных систем
Практическое занятие 7.

Вид практического занятия**:** ***подготовка доклада.***
Образовательные технологии: ***групповая дискуссия.***

Вид практического занятия**:** *смешанная форма практического занятия.*
Тема и содержание практического занятия:
Цель работы: Ознакомиться с проблемами информационных систем.

Основные положения темы занятия:

1. Разработка экспертных систем и Технология их применения.
2. Мероприятия по предотвращению угроз безопасности информационных систем

Вопросы для обсуждения:

Основной доклад (реферат) по теме занятия.

1. Области применения экспертных систем.
2. Уязвимость экспертных систем.
3. Проблемы обеспечения безопасности информационных систем.
4. Основные подходы в создании защищённых информационных систем.

продолжительность занятия – 3/2

Тема 8: Организационно-правовые аспекты обеспечения информационной безопасности информационных систем. Комплексный (системный) подход в обеспечении информационной безопасности информационных систем

Практическое занятие 8.

Вид практического занятия**:** ***подготовка доклада.***

Образовательные технологии: ***групповая дискуссия.***

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические навыки в обеспечении информационной безопасности информационных систем.

Основные положения темы занятия:

1. Правовые аспекты информационного обмена в глобальных сетях.
2. Основные стадии жизненного цикла системы защиты информации.

Вопросы для обсуждения:

Основной доклад (реферат) по теме занятия.

1. Глобальные информационные сети и системы, их свойства
2. Роль стандартов информационной безопасности при создании информационных систем.
3. Комплексный (системный) подход в обеспечении информационной безопасности информационных систем

продолжительность занятия – 3/2

Тема 9: Методы и средства обеспечения информационной безопасности информационных систем

Практическое занятие 9.

Вид практического занятия**:** ***подготовка доклада.***

Образовательные технологии: ***групповая дискуссия.***

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Ознакомиться с методами и средствами обеспечения информационной безопасности информационных систем.

Основные положения темы занятия:

1. Методы и средства защиты информации в информационных системах
2. Пути решения проблем защиты информации в информационных системах.

Вопросы для обсуждения:

Основной доклад (реферат) по теме занятия.

1. Два подхода к проблеме обеспечения информационной безопасности информационных систем
2. Задачи управления средствами информационной безопасности.
3. Политики безопасности.
4. Протоколы безопасной передачи данных.

продолжительность занятия – 8/8

5. Указания по проведению самостоятельной работы студентов

№ п/п	Наименование блока (раздела) дисциплины	Виды СРС
1.	**Тема 6: Информационные базы и банки данных. Базы знаний. Цели и задачи технологического обеспечения. Режимы обработки информации**	***Подготовка докладов по темам:*** Задача стандартизации при разработке систем защиты информации. Правовая основа защиты информации на объектах информатизации. Криптографические методы защиты информации в современных информационных системах. Компьютерные вирусы и проблемы антивирусной защиты.
2.	**Тема 7: Экспертные информационные системы. Проблемы безопасности информационных систем**	***Подготовка докладов по темам:*** Организация защиты при обмене данными в информационных системах. Протоколы, применяемые для защиты информации в сетевых информационных системах. Проблемы обеспечения информационной безопасности беспроводных информационных систем.
3	**Тема 8: Организационно-правовые аспекты обеспечения информационной безопасности информационных систем. Комплексный (системный) подход в обеспечении информацион-**	***Подготовка докладов по темам:*** Общая методология выбора средств и способов защиты информации в информационных системах. Организация парольной защиты в информационных системах.

	ной безопасности информационных систем	
4	**Тема 9: Методы и средства обеспечения информационной безопасности информационных систем**	***Подготовка докладов по темам:*** Виды атак на сетевые информационные системы и методы борьбы с ними. Скорость передачи информации дискретных каналов с помехами. Современные системы электронного документооборота и показатели их защищённости. Информационная безопасность электронного бизнеса. Оптимальные алгоритмы обработки конфиденциальной информации в сетевых информационных системах. Методы оценки эффективности функционирования современных информационных систем. Перспективные информационные системы, технологии управления и обеспечение их безопасности. Методы разграничения доступа в информационных системах. Интегрированные и корпоративные информационные системы, проблемы их защищённости. Статистические критерии обнаружения и распознавания информации.

1. Указания по проведению контрольных работ для студентов факультета заочного обучения

5.1. Требования к структуре

Структура контрольной работы должна способствовать раскрытию темы: иметь титульный лист, содержание, введение, основную часть, заключение, список литературы.

5.2. Требования к содержанию (основной части)

1. Во введении обосновывается актуальность темы, определяется цель работы, задачи и методы исследования.
2. При определении целей и задач исследования необходимо правильно их формулировать. Так, в качестве цели не следует употреблять глагол «сделать». Правильно будет использовать глаголы «раскрыть», «определить», «установить», «показать», «выявить» и т.д.
3. Основная часть работы включает 2-4 вопроса, каждый из которых посвящается решению задач, сформированных во введении, и заканчивается констатацией итогов.
4. Приветствуется иллюстрация содержания работы таблицами, графическим материалом (рисунками, схемами и т.п.).
5. Необходимо давать ссылки на используемую литературу.
6. Заключение должно содержать сделанные автором работы выводы, итоги исследования.
7. Вслед за заключением идет список литературы, который должен быть составлен и оформлен с установленными требованиями. Если в работе

имеются приложения, они оформляются на отдельных листах, и должны быть соответственно пронумерованы.

5.3. Требования к оформлению

Объём контрольной работы – 5-6 страниц формата А 4, напечатанного с одной стороны текста (1,5 интервал, шрифт Times New Roman).

5.4. Примерная тематика контрольных работ:

1. Задача стандартизации при разработке систем защиты информации.
2. Правовая основа защиты информации на объектах информатизации.
3. Криптографические методы защиты информации в современных информационных системах.
4. Компьютерные вирусы и проблемы антивирусной защиты.
5. Организация защиты при обмене данными в информационных системах.
6. Протоколы, применяемые для защиты информации в сетевых информационных системах.
7. Проблемы обеспечения информационной безопасности беспроводных информационных систем.
8. Общая методология выбора средств и способов защиты информации в информационных системах.
9. Организация парольной защиты в информационных системах.

6. Перечень основной и дополнительной учебной литературы

Основная литература:

1.Чернышев, А. Б. Теория информационных процессов и систем : учебное пособие / А. Б. Чернышев, В. Ф. Антонов, Г. Б. Суюнова. — Ставрополь : СКФУ, 2015. — 169 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/155262 (дата обращения: 23.12.2022). — Режим доступа: для авториз. пользователей.

2.Овсянников, А. С. Теория информационных процессов и систем : учебник / А. С. Овсянников. — Самара : ПГУТИ, 2019. — 274 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/223301 (дата обращения: 23.12.2022). — Режим доступа: для авториз. пользователей.

Дополнительная литература:

3.Теория информационных процессов и систем : учебное пособие. — Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2016 — Часть 1 — 2016. — 67 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/180067 (дата обращения: 23.12.2022). — Режим доступа: для авториз. пользователей.

4.Теория информационных процессов и систем : учебное пособие. — Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2016 — Часть 2 — 2016. — 87

с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/180064 (дата обращения: 23.12.2022). — Режим доступа: для авториз. пользователей.

7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

Интернет-ресурсы:

1. http://eup.ru/catalog/all-all.asp **– научно-образовательный портал.**
2. http://informika.ru/ **– образовательный портал.**
3. www.wikIsec.ru **- Энциклопедия информационной безопасности. – Публикации, статьи.**
4. **www.biblioclub.ru** - Универсальная библиотека онлайн.
5. **www.rucont.ru** - ЭБС «Руконт».
6. http://www.academy.it.ru/ **- академия АЙТИ.**
7. http://www.minfin.ru **- Официальный сайт Министерства финансов Российской Федерации**
8. http://www.gov.ru/ **- Официальный сервер органов государственной власти Российской Федерации**.
9. http://www.fsb.ru/ **- Официальный сайт Федеральной Службы Безопасности**
10. http://www.fstec.ru/ **- Официальный сайт Федеральной Службы по Техническому Экспортному контролю**

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю)

Перечень программного обеспечения: MSOffice, PowerPoint.

Информационные справочные системы:

1.Электронные ресурсы образовательной среды Университета.

2.Рабочая программа и методическое обеспечение по дисциплине: «Информационные процессы и системы как объекты информационной безопасности».