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

Троицкий Александр Витальевич
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.Б.15.09 «МОДЕЛИРОВАНИЕ ПРОЦЕССОВ И СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ»

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: Соляной В.Н. Рабочая программа дисциплины: «Моделирование процессов и систем защиты информации». – 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 29.05.2023			

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:

1. приобретение студентами знаний и представлений об основных математических подходах к изучению общих проблем информационной безопасности;
2. приобретение студентами теоретических сведений и практических навыков, позволяющих использовать математические методы и модели в системах информационной безопасности различного профиля.

В процессе обучения студент приобретает и совершенствует следующие компетенции:

В процессе обучения студент приобретает и совершенствует

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

Основными **задачами** дисциплины являются

1. освоение студентами теоретических методов дисциплины, применяемых при анализе систем, обеспечивающих информационную безопасность;
2. получение студентами умений и навыков, применяемых для решения практических задач информационной безопасности.

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 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 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 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 «Моделирование процессов и систем защиты информации» относится к обязательной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Конфиденциальное делопроизводство и защищенный электронный документооборот», «Физическая защита информационных объектов», «Основы управления информационной безопасностью», «Информационные процессы и системы как объекты информационной безопасности» и компетенциях: ДОПК-1,2,3,4; ОПК-5,10.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Информационно-аналитическая деятельность по обеспечению комплексной безопасности», «Экономика информационной безопасности», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

3.Объем дисциплины (модуля) и виды учебной работы

Общая трудоемкость дисциплины для студентов очной формы составляет 3 зачетных единицы, 108 часов; для студентов очно - заочной формы составляет 3 зачетных единицы, 108 часов.

Таблица1

Виды занятий	Всего часов	Семестр 8	Семестр 7	Семестр …	Семестр …
Общая трудоемкость	108	108			
ОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	48	48			
Лекции (Л)	12	12			
Практические занятия (ПЗ)	36	36			
Лабораторные работы (ЛР)					
Другие виды контактной работы	**10**	**10**			
Самостоятельная работа	52	52			
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	Зачет	Зачет			
ОЧНО - ЗАОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	28		28		
Лекции (Л)	12		12		
Практические занятия (ПЗ)	16		16		
Лабораторные работы (ЛР)					
Самостоятельная работа	80		80		
Другие виды контактной работы	**10**		**10**		
Практическая подготовка	**нет**		**нет**		
Курсовые работы (проекты)	-		-		
Расчетно-графические работы	-		-		
Контрольная работа, домашнее задание	+		+		
КСР	-		-		
Вид итогового контроля	Зачет		Зачет		

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	Практическая подготовка, час	Код компетенций
Тема 1. Имитационное моделирование	1/1	4/2	1/1	ДОПК-1
Тема 2. Моделирование операций по схеме марковских случайных процессов	1/1	4/2	1/1	ДОПК-1
Тема 3. Системы массового обслуживания и их применение в моделировании	1/1	4/2	1/1	ДОПК-1
Тема 4. Информационные технологии региона как объект информационной безопасности	1/1	4/2	1/1	ДОПК-1
Тема 5. Нормативно-правовые основы защиты информационных технологий	2/2	4/2	2/1	ДОПК-4
Тема 6. Защищённые информацион	2/2	4/2	2/1	ДОПК-4

ные технологии в государственном и муниципальном управлении				
Тема 7. Защищённые информационные технологии в управлении коммерческими структурами	2/2	6/2	2/2	ДОПК-4
Тема 8. Организационно-технические методы защиты информационных технологий	2/2	6/2	2/2	ДОПК-4
Итого	12/12	36/16	12/10	

4.2. Содержание тем дисциплины

Тема 1. Имитационное моделирование

Понятие численного эксперимента. Датчики случайных чисел. Имитационное моделирование. Метод Монте-Карло. Построение статистических моделей, общие оценки их качества. Построение моделей на основе нечёткой логики. Компьютерные системы символьных вычислений (EXCEL, MATHCAD, MAPLE, MATEMATICA). Основные принципы работы в этих средах. Возможности пакетов символьных вычислений. Задачи, решаемые с помощью пакетов символьных вычислений.

Тема 2. Моделирование операций по схеме марковских случайных процессов

Марковский случайный процесс с дискретными состояниями. Граф состояний. Марковская цепь. Переходные вероятности. Вероятности состояний. Уравнения Колмогорова для вероятностей состояния. Предельные вероятности состояния. Поток событий. Интенсивность потока. Стационарный поток. Поток без последействия. Простейший поток и его характеристики. Поток Пальма. Потоки Эрланга и их характеристики. Процессы «гибели и размножения». Расчет предельных вероятностей состояний. Циклические процессы. Расчет предельных вероятностей состояний. Ветвящиеся циклические процессы. Приближенное сведение немарковских процессов к марковским. Метод «псевдосостояний».

Тема 3. Системы массового обслуживания и их применения в моделировании

Понятие системы массового обслуживания. Классификация систем массового обслуживания. Основные характеристики систем массового обслуживания. Показатели эффективности работы систем массового обслуживания. Системы массового обслуживания с отказами. Системы массового обслуживания с ожиданием. Системы массового обслуживания с очередью. Применение систем массового обслуживания в моделировании.

Тема 4. Информационные технологии региона как объект информационной безопасности

Стратегический менеджмент, как система поведения предприятия на длительный период времени. Специфика информационного взаимодействия функциональных задач стратегического менеджмента. Информационные технологии стратегического менеджмента на предприятии. Реализация задач стратегического менеджмента с использованием специализированных компьютерных систем экономического и финансового моделирования. Информационные технологии решения задач финансового менеджмента и их основные процедуры. Основные принципы построения информационных систем управления персоналом в условиях корпоративных организаций. Информационные технологии по использованию трудовых ресурсов и рабочего времени в корпоративных организациях.

Тема 5. Нормативно-правовые основы защиты информационных технологий

Реализация теоретических и организационных принципов создания и функционирования информационных технологий в органах государственного и регионального управления. Информационно-вычислительные и ситуационные центры, их роль в государственном и региональном управлении. Особенности организации информационных технологий в муниципальном управлении. Информационное и технологическое обеспечение решения функциональных задач муниципального управления. Организация государственных информационных ресурсов России.

Тема 6. Защищённые информационные технологии в государственном и муниципальном управлении

Необходимость обеспечения безопасности информационных технологий. Виды угроз безопасности информационных технологий и их характеристика. Формы атак на объекты информационных систем региона. Основные методы и средства защиты информации. Оценка безопасности информационных технологий, анализ угроз и каналов утечки информации. Анализ рисков и управление ими при использовании защищённых информационных технологий. Характеристика основных методов и средств построения систем информационной безопасности региона. Особенности защиты информации в корпоративных сетях.

Тема 7. Защищённые информационные технологии в управлении коммерческими структурами

Организационные способы противодействия телефонному пиратству. Ограничение доступа к телефонным линиям связи. Основные рекомендации абонентам в случае обнаружения самовольного подключения. Характеристика современных пассивных устройств технического противодействия телефонному пиратству. Специализированные анализаторы телефонных линий связи. Краткий обзор зарубежных приборов для контроля состояния телефонных линий. Особенности активных устройств технического противодействия телефонному пиратству. Критерии оценки систем закрытия речи. Основные тенденции развития систем закрытия речи. Характеристика современных методов

противодействия утечке компьютерной и аудио видео информации.

Тема 8. Организационно-технические методы защиты информационных технологий

Компьютерная безопасность. Решение задач безопасности речевой связи с помощью компьютерных информационных технологий. Представление речевых сигналов в виде графических образов. Компьютерные технологии безопасности связи на основе цифровой обработки изображений стенограмм. Технологии обеспечения безопасности на основе индивидуальных особенностей человека. Характеристика современных методов биометрической идентификации личности. Стеганографическая защита информации цифровыми водяными знаками. Характеристика современных систем цифровых водяных знаков. Обзор основных атак на системы цифровых водяных знаков.

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 «Моделирование процессов и систем защиты информации» приведена в Приложении 1.

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

Основная литература:

1.Математическое моделирование технических систем: учебник / В.П. Тарасик. — Минск: Новое знание; М.: ИНФРА-М, 2018. — 592 с. — (Высшее образование: Бакалавриат) [электронный ресурс] // Режим доступа: http://znanium.com/catalog/product/952123

2.Аверченков В.И. Основы математического моделирования технических систем / В.И. Аверченков, В.П. Федоров, М.Л. Хейфец. – 3-е изд., стер. – Москва: Издательство «Флинта», 2016. – 271 с.: схем., ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=93344

Дополнительная литература:

3. Голубева Н. В. Математическое моделирование систем и процессов: учебное пособие / Н. В. Голубева. — 2-е изд., стер. — Санкт-Петербург: Лань, 2016. — 192 с. — ISBN 978-5-8114-1424-6. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/76825

4.Волкова В.Н., Денисов А.А. Теория систем и системный анализ. Учебник / В.Н. Волкова, А.А. Денисов. - М.:Юрайт. - 2015. - 616 с. http://www.biblio-online.ru/thematic/?8&id=urait.content.96A5D918-229B-4975-993A-3F766622372B&type=c_pub

5.Попов А.М., Сотников В.Н. Экономико-математические методы и модели. Учебник / А.М. Попов, В.Н. Сотников. - М.:Юрайт. - 2015. - 345 с. http://www.biblio-online.ru/thematic/?20&id=urait.content.C7E8DCBD-2726-402A-9854-D1C553E34796&type=c_pub

6.Гончаров В.А. Методы оптимизации. Учебное пособие для бакалавриата и магистратуры / В.А. Гончаров. - М.:Юрайт. - 2015. - 191 с. http://www.biblio-online.ru/thematic/?6&id=urait.content.780852A5-F757-48E8-BAD7-4AE3F88CBAAB&type=c_pub

7.Гришина, Наталия Васильевна. Информационная безопасность предприятия : Учебное пособие / Наталия Васильевна. - 2 ; доп. - Москва ; Москва : Издательство "ФОРУМ" : ООО "Научно-издательский центр ИНФРА-М", 2016. - 240 с. - ISBN 978-5-00091-007-8. URL: http://znanium.com/go.php?id=544554

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. **http://www.academy.it.ru/ –** академия АЙТИ.

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:

Электронные ресурсы образовательной среды Университета.

Информационно-справочные системы (Консультант+; Гарант).

Ресурсы информационно-образовательной среды Университета:

Рабочая программа и методическое обеспечение по курсу «Моделирование процессов и систем защиты информации ».

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 современными 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

«МОДЕЛИРОВАНИЕ ПРОЦЕССОВ И СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ»

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 компе-тенции	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	Тема:1,-8	- 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	- 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	- 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

				- 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	для нейтрализации определенного вида угроз - владеет навыками выбора и применения современных аппаратных и программных средств технической защиты информации	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 - знает методы хранения, обработки и передачи и получения информации из открытых информационных систем
2.	ДОПК-4	Способен проводить аудит защищенности объекта	Тема: 1-8	- владеет навыками составления отчётов по результатам	- умеет определять объекты аудита, критерии и	- знает стандарты и критерии в области аудита ИБ

		информатизации в соответствии с нормативными документами		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	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	- 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

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-1,4	***Доклад***	***А) полностью сформирована (компетенция освоена на <u>высоком</u> уровне) – 5 баллов*** ***Б) частично сформирована:*** • ***компетенция освоена на <u>продвинутом</u> уровне – 4 балла;*** • ***компетенция освоена на <u>базовом</u> уровне – 3 балла;*** ***В) не сформирована (<u>компетенция не сформирована</u>) – 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-1,4	***Выполнение контрольной работы***	***А) полностью сформирована (компетенция освоена на <u>высоком</u> уровне) – 5 баллов*** ***Б) частично сформирована:*** • ***компетенция освоена на <u>продвинутом</u> уровне – 4 балла;*** • ***компетенция освоена на <u>базовом</u> уровне – 3 балла;*** ***В) не сформирована (<u>компетенция не сформирована</u>) – 2 и***	***При определении сформированности компетенций критериями оценивания выступают методические рекомендации, разработанные по дисциплине для данного вида***

		менее баллов	

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. Характеристика защищённых технологий систем кабельного телевидения, понятие телеохраны в современном мире.
2. Основы защищённых технологий при обеспечении безопасности персонала и пользователей почтовой связи.
3. Защищённые технологии и особенности их применения в системах наблюдения дальнего действия.
4. Защищённые технологии читающих автоматов и особенности их использования в системе безопасности предприятий, фирм.
5. Характеристика современных технологий охраны объектов и основные направления их развития.
6. Основные проблемы применения защищённой технологии «речевая подпись» и пути их решения в современном мире.
7. Средства обнаружения и системы охранной сигнализации, применяемые в рамках защищённых информационных технологий предприятий и фирм.
8. Характеристика основных устройств противодействия съёму информации в муниципальных защищаемых помещениях.
9. Особенности применения защитных технологий читающе-опознающих автоматов в невидимых диапазонах электромагнитного спектра телевидения.
10. Защищённые технологии в системе обеспечения безопасности коммерческих объектов.
11. Новые возможности использования технологий стеганографии в системах цифрового телевидения.
12. Методы охраны и защиты конфиденциально ориентированного предприятия на основе применения нейро-сетевых технологий обработки информации.
13. Современные подходы в развитии биометрических технологий защиты и перспективы их развития.
14. Идентификация пользователей вычислительных систем на основе современных речевых технологий и методов искусственного интеллекта.

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

Формой контроля знаний по дисциплине «Моделирование процессов и систем защиты информации» являются две текущие аттестации в виде тестов и итоговая аттестация в виде экзамена.

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-1,4	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	тестирование	ДОПК-1,4	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	ДОПК-1,4	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	«У**довлетвори-тельно**»: • демонстрирует частичные знания по темам дисциплин; • незнание неумение использовать и применять полученные знания на практике; • не работал на практических занятиях; «**Неудовлетвор и-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:

ЗАДАНИЕ НА ВЫБОР ОДНОГО ПРАВИЛЬНОГО ВАРИАНТА ОТВЕТА

1. Какой вид входной информации используется на первом этапе системно-информационного подхода к преобразованию информации в стратегиче-

ском менеджменте?
- информация на основе сформулированной идеи стратегического менеджмента;
- информация, поступающая из внешней и внутренней среды предприятия;
- информация о стратегических задачах и достижении целевых установок;
- аналитическая информация о результатах планирования деятельности предприятия.

2. Выберите основные пакеты прикладных программ, реализующих задачи стратегического менеджмента на предприятии:
- Comfar;
- Propspin;
- WorkFlow;
- Project expert.

3. Выберите информационно-вычислительные системы, которые в настоящее время применяются для информационного обслуживания органов федерального управления:
- информационная телекоммуникационная система статистики (ИТКСС);
- система управления электронными документами (Босс-Референт);
- система технологической обработки статистической информации (СТОСИ/ЭПС);
- система автоматизированных банков экономической информации.

4. Что понимается под компьютерной стегологией?
- скрытие самого факта передачи сообщения по открытым каналам связи;
- скрытая передача условных знаков или конфиденциальной информации под видом открытой передачи данных по общедоступным каналам связи;
- компьютерное дешифрирование зашифрованных участков сообщения;
- метод кодирования сообщения с помощью криптографических алгоритмов.

5. Что понимается под сонограммой аудиосигнала?
- изображение графического образа звукового сигнала;
- изображение графического образа речи;
- изображение спектра электромагнитного сигнала;
- изображение фонообъекта звукового сигнала.

6. Входит ли блок стегокодера в систему цифровых водяных знаков?
- да;
- нет;

1.2.Типовые вопросы, выносимые на зачет

1. Сущность стратегического менеджмента на предприятиях в фирмах.
2. Функциональные задачи стратегического менеджмента и их реализация в условиях информационных технологий.
3. Какой вид входной информации используется на первом этапе преобразова-

ния информации стратегического менеджмента?
4. Информационные технологии стратегического менеджмента на предприятиях, в фирмах.
5. Основные пакеты прикладных программ, реализующих задачи стратегического менеджмента на предприятиях, в фирмах и их характеристика.
6. Программное обеспечение финансовых решений на предприятиях, в фирмах.
7. Информационные технологии решения задач финансового менеджмента.
8. Характеристика основных элементов управляющей подсистемы финансового менеджмента.
9. Комплекс задач финансового менеджмента и их особенности, виды информации, использующиеся, при решении этих задач.
10. Классификация программных средств финансового менеджмента, какие средства используются для решения задач финансового анализа?
11. Общие черты комплексных систем автоматизации управления финансово-хозяйственной деятельностью предприятий, фирм.
12. Особенности задач по оценке инвестиционных проектов и основные этапы их решения.
13. Основные особенности программных продуктов «Project Expert» и «Альт-Инвест» для решения задач финансового анализа и прогнозирования.
14. Общие технологические принципы решения задач управления персоналом в корпоративных организациях.
15. Основные подсистемы автоматизированной информационной системы управления персоналом и их характеристика.
16. Основные направления анализа информации в области управления персоналом на предприятиях, в фирмах.
17. Информационно-вычислительные и ситуационные центры в государственном и муниципальном управлении.
18. Информационные технологии решения функциональных задач в муниципальном управлении.
19. Государственные информационные ресурсы России и их характеристика.
20. Информационные ресурсы федеральных и муниципальных органов власти как объекты защиты информации.
21. Информационные ресурсы и технологии в сфере финансов и внешнеэкономической деятельности страны.
22. Информационные ресурсы отраслей материального производства, государственной системы статистики и социальной сферы, их особенности.
23. Основные виды угроз безопасности информационных систем и технологий, их характеристика.
24. Основные формы атак на объекты информационных систем предприятий, фирм и их особенности.
25. Анализ основных угроз и каналов утечки информации на предприятии в фирме, их особенности.
26. Характеристика современных методов и средств защиты информационных

технологий на предприятиях в фирмах.
27. Основные методы и средства построения систем информационной безопасности предприятий, фирм, характеристика их структурных элементов.
28. Защита информации в корпоративных сетях управления муниципалитета.
29. Анализ возможных рисков применяемых информационных технологий и управление рисками.
30. Особенности стратегии защиты информации с использованием системного подхода, комплексных решений и принципа интеграции в защищённых информационных технологиях.
31. Организационные способы противодействия телефонному пиратству на предприятиях, в фирмах.
32. Ограничение доступа к телефонным линиям связи и основные рекомендации абонентам в случае обнаружения самовольного подключения.
33. Характеристика современных пассивных устройств технического противодействия телефонному пиратству.
34. Специализированные анализаторы телефонных линий связи и их характеристика.
35. Обзор характеристик основных зарубежных приборов для контроля состояния телефонных линий.
36. Особенности активных устройств технического противодействия телефонному пиратству.
37. Основные критерии оценки систем закрытия речи и передовые тенденции развития этих систем.
38. Характеристика современных методов противодействия утечке компьютерной и аудиовидеоинформации.
39. Особенности применения современных сканирующих приёмников и индикаторов поля.
40. Характеристики и примеры использования многофункциональных поисковых систем и устройств защиты.
41. Основные характеристики и примеры использования выжигателей закладных устройств, обнаружителей и подавителей диктофонов, других высокочастотных электронных устройств.
42. Характеристики и примеры использования современных систем виброакустического зашумления помещений и сетей.
43. Организация защиты объектов от встроенных и узконаправленных микрофонов.
44. Организация защиты объектов от лазерных прослушивающих устройств.
45. Характеристика и особенности применения современных нелинейных радиолокаторов.
46. Решение задач безопасности речевой связи с помощью компьютерных информационных технологий.
47. Особенности представления речевых сигналов в виде графических образов.
48. Компьютерные технологии безопасности связи на основе цифровой обработки изображений сонограмм.

49. Технологии обеспечения безопасности на предприятии в фирме на основе индивидуальных особенностей человека.
50. Характеристика современных методов биометрической идентификации личности и их особенности.
51. Представление речевого сигнала сообщения в виде графических образов.
52. Реализация способов аудиомаркирования с помощью компьютерных технологий.
53. Основные рекомендации по практическому применению технологии «речевая подпись».
54. Стеганографическая защита информации цифровыми водяными знаками.
55. Характеристика современных систем цифровых водяных знаков и их особенности.
56. Характеристика и особенности основных атак на системы цифровых водяных знаков.
57. Особенности применения крипто-технологий в цифровом телевидении.
58. Основные рекомендации по практическому применению стеганографической технологии в цифровом телевидении.
59. Маркирование и защита интеллектуальной собственности в России.
60. Организация и методика экспресс-поиска устройств несанкционированного съёма информации.

**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)

«МОДЕЛИРОВАНИЕ ПРОЦЕССОВ И СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ»

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

Целями изучения дисциплины является: формирование у студентов специализированной базы знаний по фундаментальным проблемам информационной безопасности в условиях становления современного информационного общества, использовании организационно-правовых механизмов обеспечения конституционных прав и свобод граждан в информационной сфере, регламентирующих создание и использование защищённых информационных технологий, а также получение первичных навыков в применении защищённых технологий при обеспечении информационной безопасности различных объектов.

Задачами дисциплины является:

1. Теоретические основы подготовки студентов в области информационных технологий
2. Практические аспекты формирования подходов к выполнению самостоятельных исследований студентами в области информационных технологий

2. Указания по проведению практических занятий

Тема 1-2. Имитационное моделирование. Моделирование операций по схеме марковских случайных процессов

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: Получить практические знания и навыки моделирования основных угроз безопасности для информационного объекта.

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Информационные ресурсы библиотечной сети России.
2. Ресурсы государственной системы экономической и научно-технической информации.
3. Российские ресурсы правовой информации.
4. Информационные ресурсы федеральных и муниципальных органов власти.

Продолжительность занятия: 7/7

Тема 3-4. Системы массового обслуживания и их применение в моделировании. Информационные технологии региона как объект информационной безопасности

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: Получить практические знания и навыки моделирования основных угроз безопасности для информационного объекта.

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Информационные ресурсы в сфере финансов и внешнеэкономической деятельности государства.
2. Информационные ресурсы отраслей материального производства.
3. Информационные ресурсы государственной системы статистики.
4. Информационные ресурсы социальной сферы.

Продолжительность занятия: 7/7

Тема 5-6. Нормативно-правовые основы защиты информационных технологий. Защищённые информационные технологии в государственном и муниципальном управлении

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: Получить практические знания и навыки моделирования основных угроз безопасности для информационного объекта.

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Классификация угроз безопасности информационным объектам.
2. Основные формы атак на объекты информационных систем и технологий.
3. Анализ угроз и каналов утечки информации на информационных объектах.
4. Анализ рисков и управление ими при использовании защищённых инфомационных технологий.

Продолжительность занятия: 7/7

Тема 7. Защищённые информационные технологии в управлении коммерческими структурами

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 практические знания и навыки моделирования основных угроз безопасности для информационного объекта.

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Создание системы защиты информации в корпоративной сети управления.
2. Основные этапы разработки систем защиты информационных систем и технологий и их характеристика.
3. Проблемы защиты интеллектуальной собственности на предприятиях, в фирмах.
4. Основные направления совершенствования защищённых информационных технологий.

Продолжительность занятия: 7/7

Тема 8. Организационно-технические методы защиты информационных технологий

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 практические знания и навыки моделирования основных угроз безопасности для информационного объекта.

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Современные индикаторы поля и сканирующие приёмники.
2. Характеристика многофункциональных поисковых систем.
3. Выжигатели скрытых закладных устройств.
4. Обнаружители и подавители диктофонов и других высокочастотных электронных устройств.

Продолжительность занятия: 8/8

Указания по проведению лабораторных работ (нет в учебном плане)

Тема 1-3. Имитационное моделирование. Моделирование операций по схеме марковских случайных процессов.Системы массового обслуживания и их применение в моделировании

Лабораторные занятия 1. Метод Монте-Карло

Обсуждение понятий и решение задач на следующие темы:

1. Понятие численного эксперимента. Датчики случайных чисел.
2. Имитационное моделирование. Метод Монте-Карло.

Лабораторные занятия 2. Статистические модели. Модели, построенные на основе нечёткой логики

Обсуждение понятий и решение задач на следующие темы:

1. Построение статистических моделей, общие оценки их качества.
2. Построение моделей на основе нечёткой логики.

Лабораторные занятие 3. Компьютерные системы символьных вычислений EXCEL и MATHCAD. Применения этих систем

Обсуждение понятий и решение задач на следующие темы:

1. Возможности пакетов символьных вычислений EXCEL и MATHCAD.
2. Задачи, решаемые с помощью пакетов символьных вычислений EXCEL и MATHCAD.

Лабораторные занятия 4. Компьютерные системы символьных вычислений MAPLE и MATEMATICA. Применения этих систем

Обсуждение понятий и решение задач на следующие темы:

1. Возможности пакетов символьных вычислений MAPLE и MATEMATICA.
2. Задачи, решаемые с помощью пакетов символьных вычислений MAPLE и MATEMATICA.

Продолжительность занятия: 2/0.5

Тема 4-6. Информационные технологии региона как объект информационной безопасности. Нормативно-правовые основы защиты информационных технологий. Защищённые информационные технологии в государственном и муниципальном управлении.

Лабораторные занятия 1. Марковские случайные процессы

Обсуждение понятий и решение задач на следующие темы:

1. Марковский случайный процесс с дискретными состояниями.
2. Граф состояний.

Лабораторные занятия 2. Марковские цепи

Обсуждение понятий и решение задач на следующие темы:

1. Марковская цепь. Переходные вероятности.
2. Вероятности состояний.

Лабораторные занятия 3. Марковские цепи

Обсуждение понятий и решение задач на следующие темы:

1. Уравнения Колмогорова для вероятностей состояния.
2. Предельные вероятности состояний.

Лабораторные занятия 4. Потоки событий

Обсуждение понятий и решение задач на следующие темы:

1. Поток событий. Интенсивность потока.
2. Стационарный поток. Поток без последействия.

Лабораторные занятия 5. Потоки Пальма и Эрланга

Обсуждение понятий и решение задач на следующие темы:

1. Простейший поток и его характеристики. Поток Пальма.
2. Потоки Эрланга и их характеристики.

Лабораторные занятия 6. Процессы «гибели и размножения»

Обсуждение понятий и решение задач на следующие темы:

1. Процессы «гибели и размножения». Примеры.

2. Расчет предельных вероятностей состояний.

Лабораторные занятия 7. Циклические и немарковские процессы

Обсуждение понятий и решение задач на следующие темы:

1. Циклические процессы. Расчет предельных вероятностей состояний. Ветвящиеся циклические процессы.
2. Приближенное сведение немарковских процессов к марковским. Метод «псевдосостояний».

Продолжительность занятия: 2/0.5

Тема 7-8. Защищённые информационные технологии в управлении коммерческими структурами. Организационно-технические методы защиты информационных технологий.

Лабораторные занятия 1. Классификация систем массового обслуживания

Обсуждение понятий и решение задач на следующие темы:

1. Понятие системы массового обслуживания.
2. Классификация систем массового обслуживания.

Лабораторные занятия 2. Основные характеристики и показатели эффективности работы систем массового обслуживания

Обсуждение понятий и решение задач на следующие темы.

1. Основные характеристики систем массового обслуживания.
2. Показатели эффективности работы систем массового обслуживания.

Лабораторные занятия 3. Системы массового обслуживания с отказами.

Обсуждение понятий и решение задач на тему:
«Системы массового обслуживания с отказами».

Лабораторные занятия 4. Системы массового обслуживания с ожиданием.

Обсуждение понятий и решение задач на тему:
«Системы массового обслуживания с ожиданием».

Лабораторные занятие 5. Системы массового обслуживания с очередью.

Обсуждение понятий и решение задач на тему:
«Системы массового обслуживания с очередью».

Лабораторные занятие 6. Применение систем массового обслуживания в моделировании.

Обсуждение понятий и решение задач на тему:
«Применение систем массового обслуживания в моделировании».

Продолжительность занятия: 2/0.5

Примерный перечень вопросов к зачету

1. Понятие численного эксперимента. Примеры численных экспериментов.
2. Датчики случайных чисел.
3. Имитационное моделирование.
4. Метод Монте-Карло.
5. Построение статистических моделей, общие оценки их качества.
6. Построение моделей на основе нечёткой логики.
7. Основные принципы работы и возможности пакета EXCEL.
8. Решение конкретной задачи на компьютере в пакете EXCEL .
9. Основные принципы работы и возможности пакета MATHCAD.
10. Решение конкретной задачи на компьютере в пакете MATHCAD.
11. Основные принципы работы и возможности пакета MAPLE.
12. Решение конкретной задачи на компьютере в пакете MAPLE.
13. Основные принципы работы и возможности пакета MATEMATICA.

14. Решение конкретной задачи на компьютере в пакете MATEMATICA.
15. Марковский случайный процесс с дискретными состояниями.
16. Граф состояний Марковского процесса.
17. Марковская цепь.
18. Переходные вероятности Марковской цепи. Вероятности состояний.
19. Уравнения Колмогорова для вероятностей состояния.
20. Предельные вероятности состояния.
21. Поток событий. Интенсивность потока.
22. Стационарный поток событий. Поток без последействия.
23. Простейший поток событий и его характеристики.
24. Поток Пальма.
25. Потоки Эрланга и их характеристики.
26. Процессы «гибели и размножения».
27. Расчет предельных вероятностей состояний в процессах «гибели и размножения».
28. Циклические процессы.
29. Расчет предельных вероятностей состояний циклических процессов.
30. Ветвящиеся циклические процессы.
31. Приближенное сведение немарковских процессов к марковским.
32. Метод «псевдосостояний».
33. Понятие системы массового обслуживания.
34. Классификация систем массового обслуживания.
35. Основные характеристики систем массового обслуживания.
36. Показатели эффективности работы систем массового обслуживания.
37. Системы массового обслуживания с отказами.
38. Системы массового обслуживания с ожиданием.
39. Системы массового обслуживания с очередью.
40. Применение систем массового обслуживания в моделировании.

2.Указания по проведению самостоятельной работы студентов

№ п/п	Наименование блока (раздела) дисциплины	Виды СРС
1.	**Тема 5. Нормативно-правовые основы защиты информационных технологий**	***Подготовка докладов по темам:*** 1. Характеристика современных методов биометрической идентификации личности и их особенности. 2. Представление речевого сигнала сообщения в виде графических образов. 3. Реализация способов аудиомаркирования с помощью компьютерных технологий. 4. Основные рекомендации по практическому

		применению технологии «речевая подпись». 5. Стеганографическая защита информации цифровыми водяными знаками.
2.	**Тема 6. Защищённые информационные технологии в государственном и муниципальном управлении**	***Подготовка докладов по темам:*** 1. Характеристика современных систем цифровых водяных знаков и их особенности. 2. Характеристика и особенности основных атак на системы цифровых водяных знаков. 3. Особенности применения крипто-технологий в цифровом телевидении. 4. Основные рекомендации по практическому применению стеганографической технологии в цифровом телевидении. 5. Маркирование и защита интеллектуальной собственности в России. 6. Организация и методика экспресс-поиска устройств несанкционированного съёма информации
3	**Тема 7. Защищённые информационные технологии в управлении коммерческими структурами**	***Подготовка докладов по темам:*** 1. Характеристика защищённых технологий систем кабельного телевидения, понятие телеохраны в современном мире. 2. Основы защищённых технологий при обеспечении безопасности персонала и пользователей почтовой связи. 3. Защищённые технологии и особенности их применения в системах наблю- дения дальнего действия. 4. Защищённые технологии читающих автоматов и особенности их использо- вания в системе безопасности предприятий, фирм. 5. Характеристика современных технологий охраны объектов и основные на- правления их развития. 6. Основные проблемы применения защищённой технологии «речевая под- пись» и пути их решения в современном мире. 7. Средства обнаружения и системы охранной сигнализации, применяемые в рамках защищённых информационных технологий предприятий и фирм. 8. Характеристика основных устройств противодействия съёму информации в

		муниципальных защищаемых помещениях. 9. Особенности применения защитных технологий читающе опознающих автоматов в невидимых диапазонах электромагнитного спектра телевидения. 10. Защищённые технологии в системе обеспечения безопасности коммерческих объектов.
4	**Тема 8. Организационно-технические методы защиты информационных технологий**	***Подготовка докладов по темам:*** 11.Новые возможности использования технологий стеганографии в системах цифрового телевидения. 12. Методы охраны и защиты конфиденциально ориентированного предприятия на основе применения нейросетевых технологий обработки информации. 13. Современные подходы в развитии биометрических технологий защиты и перспективы их развития. 14. Идентификация пользователей вычислительных систем на основе современных речевых технологий и методов искусственного интеллекта.

5. Указания по проведению контрольных работ

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. Активные способы противодействия прослушиванию помещений по абонентским линиям связи.
2. Характеристика основных способов защиты абонентских телефонных линий связи от бесконтактного съёма информации.
3. Характеристика способов съёма акустической информации со стен и потолочных перекрытий охраняемых муниципальных объектов.
4. Характеристика способов съёма акустической информации с металлических труб и оконных стёкол охраняемых муниципальных объектов.
5. Характеристика способов съёма акустической информации в помещении по линии электросети охраняемых муниципальных объектов.
6. Характеристика пассивных способов противодействия прослушивания охраняемых помещений по абонентской линии связи.
7. Методика применения телефонолокационного способа съёма акустических сигналов в муниципальных защищаемых помещениях.
8. Характеристика основных устройств противодействия съёму информации в муниципальных защищаемых помещениях.
9. Основные компоненты охранной сигнализации при использовании различных датчиков.
10. Характеристика современных телевизионных средств охранной сигнализации.
11. Характеристика сетевых пассивных помехоподавляющих фильтров низких и высоких частот.
12. Методика обнаружения сигналов линейных сетевых закладок и особенности её применения.
13. Методика обнаружения оптических сигналов передатчиков ИК диапазона и особенности её применения.
14. Методика обнаружения активных прослушивающих устройств с помощью индикатора электромагнитного поля.

6. Перечень основной и дополнительной учебной литературы

Основная литература:

1.Математическое моделирование технических систем: учебник / В.П. Тарасик. — Минск: Новое знание; М.: ИНФРА-М, 2018. — 592 с. — (Высшее

образование: Бакалавриат) [электронный ресурс] // Режим доступа: http://znanium.com/catalog/product/952123
2.Аверченков В.И. Основы математического моделирования технических систем / В.И. Аверченков, В.П. Федоров, М.Л. Хейфец. – 3-е изд., стер. – Москва: Издательство «Флинта», 2016. – 271 с.: схем., ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=93344

Дополнительная литература:

3. Голубева Н. В. Математическое моделирование систем и процессов: учебное пособие / Н. В. Голубева. — 2-е изд., стер. — Санкт-Петербург: Лань, 2016. — 192 с. — ISBN 978-5-8114-1424-6. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/76825
4.Волкова В.Н., Денисов А.А. Теория систем и системный анализ. Учебник / В.Н. Волкова, А.А. Денисов. - М.:Юрайт. - 2015. - 616 с. http://www.biblio-online.ru/thematic/?8&id=urait.content.96A5D918-229B-4975-993A-3F766622372B&type=c_pub
5.Попов А.М., Сотников В.Н. Экономико-математические методы и модели. Учебник / А.М. Попов, В.Н. Сотников. - М.:Юрайт. - 2015. - 345 с. http://www.biblio-online.ru/thematic/?20&id=urait.content.C7E8DCBD-2726-402A-9854-D1C553E34796&type=c_pub
6.Гончаров В.А. Методы оптимизации. Учебное пособие для бакалавриата и магистратуры / В.А. Гончаров. - М.:Юрайт. - 2015. - 191 с. http://www.biblio-online.ru/thematic/?6&id=urait.content.780852A5-F757-48E8-BAD7-4AE3F88CBAAB&type=c_pub
7.Гришина, Наталия Васильевна. Информационная безопасность предприятия : Учебное пособие / Наталия Васильевна. - 2 ; доп. - Москва ; Москва : Издательство "ФОРУМ" : ООО "Научно-издательский центр ИНФРА-М", 2016. - 240 с. - ISBN 978-5-00091-007-8. URL: http://znanium.com/go.php?id=544554

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

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, Multisim.*

Информационные справочные системы:

1. Электронные ресурсы образовательной среды Университета
2. Информационно-справочные системы (Консультант+; Гарант).
3. Рабочая программа и методическое обеспечение по курсу «Моделирование процессов и систем защиты информации»