Государственное бюджетное образовательное учреждение высшего образования
Московской области

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

имени дважды Героя Советского Союза, летчика-космонавта А.А. Леонова

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ МОСКОВСКОЙ ОБЛАСТИ "ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ ДВАЖДЫ ГЕРОЯ СОВЕТСКОГО СОЮЗА, ЛЕТЧИКА-КОСМОНАВТА А.А.ЛЕОНОВА"

Подписано цифровой подписью: ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ МОСКОВСКОЙ ОБЛАСТИ "ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ ДВАЖДЫ ГЕРОЯ СОВЕТСКОГО СОЮЗА, ЛЕТЧИКА-КОСМОНАВТА А.А.ЛЕОНОВА"

«УТВЕРЖДАЮ»
Проректор по учебно-методической работе
И.В. Бабина
«12» апреля 2022 г.

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

Б1.Б.13.08 «МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ЗАЩИЩЕННЫХ ТКС»

Направление: 10.03.01 Информационная безопасность

Профиль: Безопасность телекоммуникационных систем (в аэрокосмической сфере)

Уровень высшего образования: бакалавриат

Квалификация (степень) выпускника: бакалавр

Форма обучения: очная

Королев
2022

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: к.в.н., доцент Соляной В.Н., к.т.н., доцент Вихров А.П. Рабочая программа дисциплины «Математическое моделирование защищенных ТКС». – Королев МО: «Технологический университет», 2022.

Рецензент: **к.в.н., доцент Сухотерин А.И.**

Рабочая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по специальности 10.03.01 «Информационная безопасность» и учебного плана, утвержденного Ученым советом МГОТУ. Протокол № 13 от 21 июня 2022 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)	2022	2023	2024	2025
Номер и дата протокола заседания кафедры	№8 от 17.03.2022			

Рабочая программа согласована:

Руководитель ОПОП ВО к.т.н., доцент Вихров А.П.

Рабочая программа рекомендована на заседании УМС:

Год утверждения (переутверждения)	2022	2023	2024	2025
Номер и дата протокола заседания УМС	Протокол № 5 от 21 июня 2022 г.			

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

Целью изучения дисциплины является:

- приобретение студентами знаний и представлений об основных математических подходах к изучению общих проблем информационной безопасности;
- 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.

ДОПК-1. Способен применять математические модели и решать задачи помехоустойчивого кодирования при проектировании защищенных телекоммуникационных систем.

ДОПК-2 Способен применять технологии защиты информации при создании защищенных телекоммуникационных систем.

ДОПК-4 Способен проводить мониторинг функционирования защищенных телекоммуникационных систем.

Показатели освоения компетенций отражают следующие индикаторы:

Трудовые действия:

ДОПК-1.15 владеет навыками выявления и устранения угроз информационной безопасности.

ДОПК-1.16 владеет навыками реализации политики информационной безопасности.

ДОПК-1.17 владеет навыками применения современных программно-аппаратных средств моделирования информационных процессов и систем ЗИ.

ДОПК-1.18 владеет навыками оценки адекватности моделей и анализа результатов моделирования.

ДОПК-2.13 владеет навыками нахождения наиболее подходящего решения применительно к заданным характеристикам информационной системы.

ДОПК-2.14 владеет навыками работы с нормативно-правовыми актами, навыками ориентации в них и поиска необходимой информации.

ДОПК-4.15 владеет навыками составления отчётов по результатам выполненного аудита.

ДОПК-4.16 владеет навыками проведения аудита ИБ со сбором данных.

ДОПК-4.17 владеет навыками по формулированию выводов и заключения по полученным результатам.

Необходимые умения:

ДОПК-1.8 умеет классифицировать информационные системы по назначению, структуре, типу.

ДОПК-1.9 умеет обосновывать решения по обеспечению информационной безопасности объектов в профессиональной сфере деятельности.
ДОПК-1.10 умеет представлять процессы в формализованном виде на языках моделирования.
ДОПК-1.11 умеет делать выводы по результатам проведённого анализа, выявляя потенциальные угрозы ИБ.
ДОПК-2.9 умеет сопоставлять основные структурно-функциональные характеристики информационных систем с требованиями руководящих документов.
ДОПК-2.10 умеет классифицировать информацию и автоматизированные системы, определять основные требования к ее защите.
ДОПК-4.9 умеет определять объекты аудита, критерии и область их действий.
ДОПК-4.10 умеет применять инструментальные средства мониторинга и аудита безопасности.

Необходимые знания:

ДОПК-1.3 знает стратегии обеспечения информационной безопасности, способы их организации и оптимизации.
ДОПК-1.4 знает определения рисков информационной безопасности применительно к объекту информатизации с заданными характеристиками.
ДОПК-1.5 знает методы и подходы к реализации системы управления безопасностью автоматизированных информационных систем.
ДОПК-2.4 знает руководящие документы в области классификации современных информационных систем и средств вычислительной и техники.
ДОПК-2.5 знает основы нормативно-правовых актов в области защиты информации конфиденциального характера.
ДОПК-4.1 знает стандарты и критерии в области аудита ИБ.
ДОПК-4.2 знает требования законодательства по обеспечению безопасности персональных данных.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Математическое моделирование защищенных систем ТКС» относится к обязательной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Защита информации в ТКС», «Беспроводные системы связи и их безопасность», «Проектирование элементов защищенных ТКС», и компетенциях: ОПК-1,6,8,12,13; ДОПК-1-4.

Дисциплина направлена на формирование следующих компетенций:

ДОПК-1. Способен применять математические модели и решать задачи помехоустойчивого кодирования при проектировании защищенных телекоммуникационных систем;

ДОПК-2. Способен применять технологии защиты информации при создании защищенных телекоммуникационных систем;

ДОПК-4. Способен проводить мониторинг функционирования защищенных телекоммуникационных систем.

Целью изучения дисциплины является профессиональная подготовка бакалавров, способных планировать и проводить математическое моделирование объектов, явлений и процессов в телекоммуникационных системах.

Задачи дисциплины:

- привить навыки постановки исследовательских задач, математического моделирования объектов, явлений и процессов;
- получение учащимися базовых знаний о методах формализации процессов функционирования систем и сетей телекоммуникаций в объеме, необходимом для построения исследуемых моделей;
- формировать у студентов знания, умения и навыки, необходимые для разработки телекоммуникационных систем.

В содержании курса раскрываются вопросы, связанные с изучением основ теории моделирования, математических схем и алгоритмов моделирования систем.

Общая трудоемкость освоения дисциплины составляет 4 зачетных единицы, 144 часа. Преподавание дисциплины ведется на 4 курсе в 8 семестре для очной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в

форме контрольной работы и экзамена в 8 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения дисциплины «Комплексное обеспечение защиты информации объекта информатизации (предприятия)», прохождения практики и выполнения выпускной квалификационной работы бакалавра.

3. Объем дисциплины (модуля) и виды учебной работы

Общая трудоемкость дисциплины для студентов очной формы составляет 4 зачетных единицы, 144 часов.

Таблица1

Виды занятий	**Всего часов**	**Семестр 8**
Общая трудоемкость	144	144
Аудиторные занятия	48	48
Лекции (Л)	12	12
Практические занятия (ПЗ)	36	36
Лабораторные работы (ЛР)	-	-
Самостоятельная работа	88	88
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

4. Содержание дисциплины

4.1. Темы дисциплины и виды занятий

Таблица 2

Наименование тем	Лекции, час. Очное	Практические занятия, час Очное	Лабораторные работы, час. Очное	Занятия в интерактивной форме, час	Код компетенций
Тема 1. Имитационно моделирование	1	4	-	-	ДОПК-1 ДОПК-2 ДОПК-4
Тема 2. Моделировани операций по схеме марковски случайных процессов	1	4	-	-	ДОПК-1 ДОПК-2 ДОПК-4
Тема 3. Системы массовог обслуживания и их применени в моделировании	1	4	-	-	ДОПК-1 ДОПК-2 ДОПК-4
Тема 4. Информационны технологии региона как объекты информационно безопасности	1	4	-	-	ДОПК-1 ДОПК-2 ДОПК-4
Тема 5. Нормативно-правовы основы защиты информационных технологий	2	4	-	-	ДОПК-1 ДОПК-2 ДОПК-4
Тема 6. Защищённые информационные технологии в государственном и муниципальном управлении	2	4	-	2	ДОПК-1 ДОПК-2 ДОПК-4
Тема 7. Защищённые информационные технологии в управлении	2	4	-	2	ДОПК-1 ДОПК-2 ДОПК-4

коммерческими структурами					
Тема 8. Организационно-технические методы защиты информационных технологий	2	6	-	2	ДОПК-1 ДОПК-2 ДОПК-4
Итого	12	36	-	6	

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 «Математическое моделирование защищенных ТКС» приведена в Приложении 1.

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

7.1 Основная литература:

1. Голубева, Н. В. Основы математического моделирования систем и процессов : учебное пособие / Н. В. Голубева. — 2-е изд., с измен. — Омск : ОмГУПС, 2019. — 95 с. — Текст : электронный // Лань : электронно-библиотечная система : [сайт] https://e.lanbook.com/book/12915 3

2. Щеглов А.Ю., Щеглов К.А. Математические модели и методы формального проектирования системы защиты информационных систем : учеб. пособие. СПб. : Университет ИТМО, 2015.

3. Фетисов Г.Г. и др. Региональная экономика и управление. Учебник. – М.: ИНФРА – М, 2007.

4. Основы управления информационной безопасностью. Учебное пособие для вузов. – 2-е изд исправ. Серия «Вопросы управления информационной безопасностью. Выпуск 1» кн. 1. А.П. Курило, Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой.- М.: Горячая линия – Телеком, 2013. - 244с.

5. Проверка и оценка деятельности по управлению информационной безопасностью. Учебное пособие для вузов. Вопросы управления информационной безопасностью кн. 5. Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия – Телеком, 2012. - 166с

6. О.А. Волгина и др. Математическое моделирование экономических процессов и систем. Уч. пособие.- 3 изд, - МКНОРУС, 2014- 200 с. (Бакалавры) SBN 978-5- 406-03252-7

7. Анисимов, А. А. Менеджмент в сфере информационной безопасности / А. А. Анисимов ; А.А. Анисимов. - Москва : Интернет-Университет Информационных Технологий, 2009. - 176 с. - (Основы информационных технологий). - ISBN 9778-5-9963-0237-6. URL: http://biblioclub.ru/index.php?page=book&id=232981

7.2 Дополнительная литература:

1. Цуканова О.А., Смирнов С.Б. Экономика защиты информации: Учебное пособие. – СПб.: СПб ГУИТМО,2007

2. Г.А. Тактаров. Финансовая среда предпринимательства и предпринимательские риски, Учебное пособие, М.: ФиС, 2008

3. 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

10.1 Перечень программного обеспечения: MSOffice, PowerPoint.

10.2 Информационные справочные системы:

1. Ресурсы информационно-образовательной среды.
2. Рабочая программа и методическое обеспечение по дисциплине: «Математическое моделирование защищенных ТКС»

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 Windows10; офисные программы MSOffice19;
- 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

«МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ЗАЩИЩЕННЫХ ТКС»

(Приложение 1 к рабочей программе)

Направление: 10.03.01 Информационная безопасность

Профиль: Безопасность телекоммуникационных систем (в аэрокосмической сфере)

Уровень высшего образования: бакалавриат

Квалификация (степень) выпускника: бакалавр

Форма обучения: очная

Королев
2022

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

№ п/п	Индекс компетенции	Содержание компетенции (или ее части)*	Раздел дисциплины, обеспечивающий формирование компетенции (или ее части)	В результате изучения раздела дисциплины, обеспечивающего формирование компетенции (или ее части), обучающийся должен:		
				Трудовые действия	Необходимые умения	Необходимые знания
1.	ДОПК-1	Способен применять математические модели и решать задачи помехоустойчивого кодирования при проектировании защищенных телекоммуникационных систем	Тема:1,3,4	ДОПК-1.15 владеет навыками выявления и устранения угроз информационной безопасности ДОПК-1.16 владеет навыками реализации политики информационной безопасности ДОПК-1.17 владеет навыками применения современных программно-аппаратных средств моделирования информационных процессов и систем ЗИ ДОПК-1.18 владеет навыками оценки адекватности моделей и анализа результатов моделирования	ДОПК-1.8 умеет классифицировать информационные системы по назначению, структуре, типу ДОПК-1.9 умеет обосновывать решения по обеспечению информационной безопасности объектов в профессиональной сфере деятельности ДОПК-1.10 умеет представлять процессы в формализованном виде на языках моделирования ДОПК-1.11 умеет делать выводы по результатам проведённого анализа, выявляя потенциальные угрозы ИБ	ДОПК-1.3 знает стратегии обеспечения информационной безопасности, способы их организации и оптимизации ДОПК-1.4 знает определения рисков информационной безопасности применительно к объекту информатизации с заданными характеристиками ДОПК-1.5 знает методы и подходы к реализации системы управления безопасностью автоматизированных информационных систем
2.	ДОПК-2	Способен применять технологии защиты информации при создании защищенных телекоммуникационных систем	Тема:2,4	ДОПК-2.13 владеет навыками нахождения наиболее подходящего решения применительно к заданным характеристикам информационной системы ДОПК-2.14	ДОПК-2.9 умеет сопоставлять основные структурно-функциональные характеристики информационных систем с требованиями руководящих документов ДОПК-2.10	ДОПК-2.4 знает руководящие документы в области классификации современных информационных систем и средств вычислительной и техники ДОПК-2.5 знает основы нормативно-правовых актов в области защиты информации

				владеет навыками работы с нормативно-правовыми актами, навыками ориентации в них и поиска необходимой информации	умеет классифицировать информацию и автоматизированные системы, определять основные требования к ее защите	конфиденциального характера
4.	ДОПК-4	Способен проводить мониторинг функционирования защищенных телекоммуникационных систем	Тема:2,3,4,5-8	ДОПК-4.15 владеет навыками составления отчётов по результатам выполненного аудита ДОПК-4.16 владеет навыками проведения аудита ИБ со сбором данных ДОПК-4.17 владеет навыками по формулированию выводов и заключения по полученным результатам	ДОПК-4.9 умеет определять объекты аудита, критерии и область их действий ДОПК-4.10 умеет применять инструментальные средства мониторинга и аудита безопасности	ДОПК-4.1 знает стандарты и критерии в области аудита ИБ ДОПК-4.2 знает требования законодательства по обеспечению безопасности персональных данных

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

Код компетенции	Инструменты, оценивающие сформированность компетенции	Показатель оценивания компетенции	Критерии оценки
ДОПК-1 ДОПК-2 ДОПК-4	Доклад в форме презентации	А) полностью сформирована **5 баллов** В) частично сформирована **3-4 балла** С) не сформирована **2 балла**	Проводится устно с использованием мультимедийных систем, а также с использованием технических средств Время, отведенное на процедуру – 10 - 15 мин. Неявка – 0. Критерии оценки: 1.Соответствие представленной презентации заявленной тематике (1 балл). 2.Качество источников и их количество при подготовке доклада и разработке презентации (1 балл). 3.Владение информацией и способность отвечать на вопросы аудитории (1 балл). 4.Качество самой представленной презентации (1 балл). 5.Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл). Максимальная сумма баллов - 5 баллов. Результаты оценочной процедуры представляются обучающимся непосредственно в день проведения презентации – для текущего контроля. Оценка проставляется в электронный журнал.
ДОПК-1 ДОПК-2 ДОПК-4	Доклад в форме презентации	А) полностью сформирована **5 баллов** В) частично сформирована **3-4 балла** С) не сформирована **2 балла**	Проводится устно с использованием мультимедийных систем, а также с использованием технических средств Время, отведенное на процедуру – 10 - 15 мин. Неявка – 0. Критерии оценки: 1.Соответствие представленной презентации заявленной тематике (1 балл). 2.Качество источников и их количество при подготовке доклада и разработке презентации (1 балл). 3.Владение информацией и способность отвечать на вопросы аудитории (1 балл). 4.Качество самой представленной презентации (1 балл).

			5.Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл). Максимальная сумма баллов - 5 баллов. Результаты оценочной процедуры представляются обучающимся непосредственно в день проведения презентации – для текущего контроля. Оценка проставляется в электронный журнал.
ДОПК-1 ДОПК-2 ДОПК-4	Доклад в форме презентации	А) полностью сформирована **5 баллов** В) частично сформирована **3-4 балла** С) не сформирована **2 балла**	Проводится устно с использованием мультимедийных систем, а также с использованием технических средств Время, отведенное на процедуру – 10 - 15 мин. Неявка – 0. Критерии оценки: 1.Соответствие представленной презентации заявленной тематике (1 балл). 2.Качество источников и их количество при подготовке доклада и разработке презентации (1 балл). 3.Владение информацией и способность отвечать на вопросы аудитории (1 балл). 4.Качество самой представленной презентации (1 балл). 5.Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл). Максимальная сумма баллов - 5 баллов. Результаты оценочной процедуры представляются обучающимся непосредственно в день проведения презентации – для текущего контроля. Оценка проставляется в электронный журнал.
ДОПК-1 ДОПК-2 ДОПК-4	Контрольная работа	А) полностью сформирована **5 баллов** В) частично сформирована **3-4 балла** С) не сформирована **2 балла**	Проводится письменно с использованием мультимедийных систем, а также с использованием технических средств Время, отведенное на процедуру – 10 - 15 мин. Неявка – 0. Критерии оценки: 1.Соответствие представленной презентации заявленной тематике (1 балл). 2.Качество источников и их количество при подготовке доклада и разработке презентации (1 балл).

			3.Владение информацией и способность отвечать на вопросы аудитории (1 балл). 4.Качество самой представленной презентации (1 балл). 5.Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл). Максимальная сумма баллов - 5 баллов. Результаты оценочной процедуры представляются обучающимся непосредственно в день проведения презентации – для текущего контроля. Оценка проставляется в электронный журнал.

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

3.1 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.

3.2 Примерная тематика заданий на контрольную работу:

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.

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

Формой контроля знаний по дисциплине «Математическое моделирование защищенных ТКС» 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
Согласно учебному плану	тестирование	ДОПК-1 ДОПК-2 ДОПК-4	20 вопросов	Компьютерное тестирование ; время отведенное на процедуру - 30 минут	Результаты тестирования предоставляются в день проведения процедуры	Критерии оценки определяются процентным соотношением. Не явка - Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%.
Согласно учебному плану	тестирование	ДОПК-1 ДОПК-2 ДОПК-4	20 вопросов	Компьютерное тестирование; время отведенное на процедуру – 30 минут	Результаты тестирования предоставляются в день проведения процедуры	Критерии оценки определяются процентным соотношением. Не явка -0 Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%. Максимальная оценка – 5 баллов.
Согласно учебному плану	Экзамен	ДОПК-1 ДОПК-2 ДОПК-4	3 вопроса	Экзамен проводится в письменной форме, путем ответа на вопросы. Время, отведенное на процедуру – 30 минут.	Результаты предоставляются в день проведения экзамена	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 «**Удовлетвори-тельно**»: • демонстрирует частичные знания по темам дисциплин; • незнание неумение использовать и применять полученные знания на практике; • не работал на практических занятиях; «**Неудовлетворительно**»: • 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.

4.1 Типовые вопросы, выносимые на тестирование

Тесты используются в режиме промежуточного контроля. По форме

заданий выбраны закрытые тесты (с выборочным ответом). Каждому вопросу соответствует один вариант ответа.

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

4.2 Типовые вопросы, выносимые на экзамен

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 преобразования 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.

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)

«МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ЗАЩИЩЕННЫХ ТКС»

(Приложение 2 к рабочей программе)

Направление: 10.03.01 Информационная безопасность

Профиль: Безопасность телекоммуникационных систем (в аэрокосмической сфере)

Уровень высшего образования: бакалавриат

Квалификация (степень) выпускника: бакалавр

Форма обучения: очная

Королев
2022

1. Общие положения

Цель 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.

Задачи дисциплины:

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**:** *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: 8

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

Практическое занятие 2.

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: 8

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

Практическое занятие 3.

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: 8

Тема 7. Защищённые информационные технологии в управлении коммерческими структурами

Практическое занятие 4.

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: 4

Тема 8. Организационно-технические методы защиты информационных технологий

Практическое занятие 5.

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: 4

3. Указания по проведению лабораторных работ

Не предусмотрены учебным планом

Примерный перечень вопросов к экзамену

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.

4. Указания по проведению самостоятельной работы студентов

Цель самостоятельной работы: подготовить студентов к самостоятельному научному творчеству.

Задачи самостоятельной работы:

1) расширить представление в области существующих современных аппаратных средств вычислительной техники;

2) привить навыки самостоятельного решения нестандартных задач в области аппаратных средств вычислительной техники.

Объем времени на самостоятельную работу, и виды самостоятельной работы представлены в таблице 1.

Таблица 1

Объем времени и виды самостоятельной работы

Виды самостоятельной работы	**Очная форма обучения**
	Всего академических часов
Всего часов на самостоятельную работу	88
Вопросы, выносимые на самостоятельное изучение	22
Подготовка к практическим занятиям	22
Подготовка к лабораторным занятиям	-
Подготовка докладов	22
Выполнение практических заданий	22

Вопросы, выносимые на самостоятельное изучение:

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.
6. Характеристика современных систем цифровых водяных знаков и их особенности.
7. Характеристика и особенности основных атак на системы цифровых водяных знаков.
8. Особенности применения криптотехнологий в цифровом телевидении.
9. Основные рекомендации по практическому применению стеганографической технологии в цифровом телевидении.
10. Маркирование и защита интеллектуальной собственности в России.
11. Организация и методика экспресс-поиска устройств несанкционированного съёма информации

Тематическое содержание самостоятельной работы представлено в таблице 2.

Таблица 2

Тематическое содержание самостоятельной работы

№ п/п	Виды самостоятельной работы	Количество часов	Перечень заданий
1.	Вопросы, выносимые на самостоятельное изучение	22	Изучение открытых источников
2.	Подготовка к практическим занятиям	22	Изучение открытых источников при подготовке доклада на выбранную тему.
3.	Подготовка к лабораторным занятиям	-	-
4.	Тематика докладов	22	Вопросы тем 1-8 практических занятий
5.	Выполнение практических заданий	22	Вопросы тем 1-8 практических занятий

Примерные темы докладов

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 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)

8.2.1. Во введении обосновывается актуальность темы, определяется цель работы, задачи и методы исследования.

8.2.2. Основная часть работы раскрывает процесс проектирования заданного аппаратного устройства и должна содержать соответствующие таблицы или временные диаграммы, которые должны формироваться разрабатываемым устройством, принципиальную схему устройства и описание его работы.

8.2.3. В процессе изложения материала необходимо давать ссылки на используемую литературу.

4. Заключение должно содержать сделанные автором работы выводы, итоги исследования.

5. Вслед за заключением идет список литературы, который должен быть составлен в соответствии с установленными требованиями.

Требования к оформлению

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

6. Перечень основной и дополнительной учебной литературы

Основная литература:

1. Голубева, Н. В. Основы математического моделирования систем и процессов : учебное пособие / Н. В. Голубева. — 2-е изд., с измен. — Омск : ОмГУПС, 2019. — 95 с. — Текст : электронный // Лань : электронно-библиотечная система : [сайт] https://e.lanbook.com/book/12915 3
2. Щеглов А.Ю., Щеглов К.А. Математические модели и методы формального проектирования системы защиты информационных систем : учеб. пособие. СПб. : Университет ИТМО, 2015.
3. Фетисов Г.Г. и др. Региональная экономика и управление. Учебник. – М.: ИНФРА – М, 2007.
4. Основы управления информационной безопасностью. Учебное пособие для вузов. – 2-е изд исправ. Серия «Вопросы управления информационной безопасностью. Выпуск 1» кн. 1. А.П. Курило, Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой.- М.: Горячая линия – Телеком, 2013. - 244с.
5. Проверка и оценка деятельности по управлению информационной безопасностью. Учебное пособие для вузов. Вопросы управления информационной безопасностью кн. 5. Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия – Телеком, 2012. - 166с
6. О.А. Волгина и др. Математическое моделирование экономических процессов и систем. Уч. пособие.- 3 изд, - МКНОРУС, 2014- 200 с. (Бакалавры) SBN 978-5- 406-03252-7
7. Анисимов, А. А. Менеджмент в сфере информационной безопасности / А. А. Анисимов ; А.А. Анисимов. - Москва : Интернет-Университет Информационных Технологий, 2009. - 176 с. - (Основы информационных технологий). - ISBN 9778-5-9963-0237-6. URL: http://biblioclub.ru/index.php?page=book&id=232981

Дополнительная литература:

1. Цуканова О.А., Смирнов С.Б. Экономика защиты информации: Учебное пособие. – СПб.: СПб ГУИТМО,2007
2. Г.А. Тактаров. Финансовая среда предпринимательства и предпринимательские риски, Учебное пособие, М.: ФиС, 2008
3. 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

Перечень программного обеспечения: *MSOffice, Multisim.*

Информационные справочные системы:

1. Ресурсы информационно-образовательной среды МГОТУ
2. Рабочая программа и методическое обеспечение по дисциплине «Математическое моделирование защищенных ТКС».