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.О.13.04 «ЗАЩИТА ИНФОРМАЦИИ В ТКС»

Направление: 10.03.01 Информационная безопасность

Профиль: Безопасность телекоммуникационных систем (в аэрокосмической сфере)

Уровень высшего образования: бакалавриат

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.т.н., доцент Вихров А.П. Рабочая программа дисциплины: «Защита информации в ТКС». – Королев МО: «Технологический университет», 2022.

Рецензент: к.в.н., доцент Соляной В.Н.

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 формирование у обучаемых специализированной базы знаний по фундаментальным проблемам информационной безопасности в условиях становления современного информационного общества, а также получение навыков в применении технологий обеспечения информационной безопасности объектов регионального уровня, а также в процессе управления информационной безопасностью защищаемых объектов.

В процессе обучения студент приобретает и совершенствует следующие компетенции.

Профессиональные компетенции:

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

ОПК-6. Способен при решении задач профессиональной деятельности организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;

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-3 Способен осуществлять эксплуатацию и проводить техническое обслуживание защищенных телекоммуникационных систем

ДОПК-4 Способен проводить мониторинг функционирования защищенных телекоммуникационных систем

Основными **задачами** дисциплины являются:

- ознакомление обучаемых с процессами анализа фундаментальных и прикладных проблем информационной безопасности в условиях становления современного информационного общества, разработка планов и программ проведения научных исследований и технических проектов, подготовка отдельных заданий для исполнителей и выполнение научных исследований по выбранной теме;
- формирование у обучаемых способности самостоятельно организовывать работу коллектива исполнителей, принятию управленческих решений в условиях спектра мнений, определению порядка выполнения работ;
- участие в работах по созданию, изготовлению, монтажу, наладке, испытаниях и сдаче в эксплуатацию систем и средств обеспечения информационной безопасности, разработке проектов методических и

нормативных документов, предложений и мероприятий по реализации разработанных проектов и программ;
формирование обучаемыми предложений по совершенствованию, модернизации, унификации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами.

Показатели освоения компетенций отражают следующие индикаторы:
Трудовые действия:
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-2.11 владеет навыками классификации информационных систем и средств вычислительной техники по требованиям регуляторов ИБ.
ДОПК-3.12 владеет навыками проведения лицензирования в области защиты информации.
ДОПК-4.16 владеет навыками проведения аудита ИБ со сбором данных.
Необходимые умения:
ОПК-1.2.1 умеет классифицировать и оценивать угрозы информационной безопасности.
ОПК-6.2.1 умеет разрабатывать модели угроз и модели нарушителя объекта информатизации.
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-2.7 умеет анализировать эффективность применения мер по обеспечению ЗИ и разрабатывать предложения по совершенствованию структуры мер и повышению эффективности.
ДОПК-3.9 умеет организовывать проведение и сопровождать аттестацию объекта информатизации в соответствии с требованиями нормативных документов.
ДОПК-4.10 умеет применять инструментальные средства мониторинга и аудита безопасности.
Необходимые знания:
ОПК-1.1.1 знает понятия информации и информационной безопасности.
ОПК-1.1.2 знает место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики.
ОПК-6.1.5 знает основные угрозы безопасности информации и модели нарушителя объекта информатизации.
ДОПК-1.2 знает технологии проектирования и построения информационных систем.

ДОПК-2.1 знает подходы к построению подсистем фиксации и реагирования на инциденты информационной безопасности.
ДОПК-3.1 знает государственные нормативные документы в области организации проведения и сопровождения аттестации объекта информатизации.
ДОПК-4.1 знает стандарты и критерии в области аудита ИБ.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Защита информации в 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: «Основы информационной безопасности», «Организационное и правовое обеспечение информационной безопасности»» и компетенциях: ОПК-1,3,5,6,8.

Дисциплина направлена на формирование следующих компетенций:

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

ОПК-6. Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;

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-3. Способен осуществлять эксплуатацию и проводить техническое обслуживание защищенных телекоммуникационных систем;

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

Курс посвящен вопросам обеспечения безопасности телекоммуникационных систем.

Цель курса - ознакомить с отечественными и зарубежными инструментами обеспечения информационной безопасности корпоративных систем.

Содержание курса включает с себя изучение сущности и задач системы защиты информации (СЗИ) телекоммуникационных систем (ТКС), факторов, влияющих на организацию СЗИ ТКС; компонентов и условий функционирования СЗИ ТКС; модели технологического и организационного построения СЗИ ТКС; кадрового, материально-технического и нормативно-методического обеспечения функционирования СЗИ ТКС; сущности и содержание контроля функционирования СЗИ ТКС; особенностей управления СЗИ ТКС и состава методов и моделей оценки эффективности СЗИ ТКС.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов. Преподавание дисциплины ведется на 3 курсе в 5 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 5 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Сети и системы передачи информации» «Беспроводные системы связи и их безопасность», «Математическое моделирование защищенных систем ТКС», прохождения практики и выполнения выпускной квалификационной работы бакалавра.

3. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины для студентов очной формы составляет 3 зачетных единицы, 108 часов.

Таблица 1

Виды занятий	Всего часов	Семестр 5
Общая трудоемкость	**108**	**108**
Аудиторные занятия	**48**	**48**
Лекции (Л)	**16**	**16**
Практические занятия (ПЗ)	**16**	**16**
Лабораторные работы (ЛР)	**16**	**16**
Самостоятельная работа	**50**	**50**
Другие виды контактной работы	**10**	**10**
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**

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

4. Содержание дисциплины

4.1.Темы дисциплины и виды занятий

Наименование тем	Лекции, час. Очное	Практические занятия, час. Очное	Лабораторные работы, час. Очное	Занятия в интерактивной форме, час. Очное	Код компетенций
Раздел 1. Общие положения, организационно-правовые и криптографические основы ЗИ					
Тема 1. Основные понятия и положения защиты информации в ин формационно-вычислительных системах и организационно-правовые меры ЗИ	**2**	**2**	**-**	**1**	**ОПК-1; ОПК-6; ДОПК-1;**
Тема 2. Стандарты и спецификации в области информационной безопасности	**2**	**2**	**-**	**1**	**ОПК-1; ОПК-6; ДОПК-1;**
Тема 3. Административный уровень информационной безопасности в инфор-мационно-вычислительной системе	**2**	**2**	**-**	**1**	**ОПК-1; ОПК-6; ДОПК-1;**
Тема 4. Криптографическая защита информации	**2**	**2**	**-**	**1**	**ДОПК-2; ДОПК-3; ДОПК-4**
Раздел 2. Безопасность ОС, программного обеспечения, корпоративных ВС и антивирусная защита					
Тема 5. Модели безопасности основных операционных систем	**2**	**2**	**-**	**2**	**ДОПК-2; ДОПК-3; ДОПК-4**
Тема 6. Системы защиты программного обеспечения	**2**	**2**	**-**	**2**	**ДОПК-2; ДОПК-3; ДОПК-4**
Тема 7. Защита информации в корпоративных сетях	**2**	**2**	**-**	**2**	**ДОПК-2; ДОПК-3; ДОПК-4**

Тема 8. Защита от информационных инфекций. Вирусология	**2**	**2**	**-**	**2**	
Итого:	**16**	**16**	**16**	**12**	

4.2 Содержание тем дисциплины

Тема 1. Основные понятия и положения защиты информации в ин формационно-вычислительных системах и организационно-правовые меры ЗИ. Предмет защиты информации. Объект защиты информации. Понятие угрозы безопасности. Классификация угроз информационной безопасности. Классификация злоумышленников. Основные методы реализации угроз информационной безопасности. Правовые и организационные методы защиты информации в информационно-вычислительных системах**.** Правовое регулирование в области безопасности информации. Государственная политика РФ в области безопасности информационных технологий. Законодательная база в области информационных технологий. Структура государственных органов, обеспечивающих безопасность информационных технологий. Общая характеристика организационных методов защиты.

Тема 2. Стандарты и спецификации в области информационной безопасности. Общие критерии безопасности. Подготовка и целевая направленность общих критериев. Организация общих критериев. Возможности и применимость. Концепции общих критериев. Действующие стандарты и рекомендации в области информационной безопасности. Критерии оценки надежных компьютерных систем («оранжевая книга» министерства обороны США). Гармонизированные критерии европейских стран. Руководящие документы по защите от несанкционированного доступа Гостехкомиссии при президенте РФ. Особенности информационной безопасности компьютерных сетей. Рекомендации X.800

Тема 3. Административный уровень информационной безопасности в информационно-вычислительной системе. Понятие политики безопасности. Анализ риска. Угрозы/видимость. Уязвимость/последствия. Учет информационных ценностей. Модели основных типов политик безопасности. Типы политик безопасности. Модель матрицы доступов Харри- Сон-Руззо-Ульмана. Модель распространения прав доступа Take-grant. Модель системы безопасности Белла-Лападула. Модель LOW-WATER-MARK. Модели ролевого разграничения доступа.

Тема 4. Криптографическая защита информации. Основные определения криптологии. Классификация методов криптографического закрытия информации. Основы теории к. Шеннона. Основные криптографические модели и алгоритмы шифрования. Симметричные

методы шифрования. Асимметричные методы шифрования. Сравнение криптографических методов. Методы кодирования.

Тема 5. Модели безопасности основных операционных систем. Механизмы защиты операционных систем. Система безопасности ос WINDOWS NT. Защита в операционной системе UNIX. Защита в операционной системе NOVELL NETWARE.

Тема 6. Системы защиты программного обеспечения. Классификация систем защиты программного обеспечения. Достоинства и недостатки основных систем защиты. Упаковщики/шифраторы. Системы защиты от несанкционированного копирования. Системы защиты от несанкционированного доступа. Показатели эффективности систем защиты.

Тема 7. Защита информации в корпоративных сетях. Основы и цель политики безопасности в компьютерных сетях. Управление доступом. Идентификация и установление подлинности. Проверка полномочий субъектов на доступ к ресурсам. Регистрация обращений к защищаемым ресурсам. Реагирование на несанкционированные действия. Многоуровневая защита корпоративных сетей. Аутентификация. Анализ возможностей маршрутизации и прокси-серверов. Типы межсетевых экранов.

Тема 8. Защита от информационных инфекций. Вирусология. Классификация компьютерных вирусов. Профилактика и лечение информационных инфекций. Программы обнаружения и защиты от вирусов.

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 «Теоретические основы компьютерной безопасности» приведена в Приложении 1.

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

7.1 Основная литература:

1. Баранова Е.К., Бабаш А.В. Информационная безопасность и защита информации : учебное пособие. Издательство: РИОР. Год издания: 2022. ISBN: 978-5-369-01761-6

2. Бондарев В.В. Введение в информационную безопасность автоматизированных систем : учебное пособие. Москва : Издательство МГТУ им. Н.Э. Баумана, 2016. ISBN 978-5-7038-4414-4

7.2 Дополнительная литература:

1. Шаньгин В. Ф. Информационная безопасность. - М.: ДМК Пресс, 2014. - 702 с.: ил. ISBN 978-5-94074-768-0
2. Оценка относительного ущерба безопасности информационной системы: Монография / Е.А. Дубинин, Ф.Б. Тебуева, В.В. Копытов. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2014. - 192 с.: ил.; Научная мысль. ISBN 978-5-369-01371-7.
3. Майкл Коллинз. Защита сетей. Подход на основе анализа данных / пер. с анг. А.В. Добровольская. –М.: ДМК Пресс, 2020. ISBN 978-5-97060-649-0

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

Интернет-ресурсы:

1. **http://www.gov.ru** - сервер органов государственной власти Российской Федерации.
2. **http://www.minfin.ru** - официальный сайт Министерства финансов Российской Федерации.
3. http://www.biblioclub.ru
4. http://znanium.com

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 МГОТУ.
2. Рабочая программа и методическое обеспечение по дисциплине: «Защита информации в 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 WindowsXP; офисные программы MSOffice 7; программы эмуляции виртуальных машин (VM-vare, VM-box или др.); операционная система MS Windows Server 2003 или др. сетевая ОС.
- рабочее место преподавателя, оснащенное компьютером с доступом в Интернет;
- рабочие места студентов, оснащенные компьютерами с доступом в Интернет.

Самостоятельная работа студентов может проводится как в специально оборудованных компьютерных классах академии с выходом в Интернет, так и в домашних условиях при наличии Интернет – сети.

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

Б1.О.13.04 «Защита информации в ТКС»
(Приложение 1 к рабочей программе)

Направление: 10.03.01 Информационная безопасность

Профиль: Безопасность телекоммуникационных систем (в аэрокосмической сфере)

Уровень высшего образования: бакалавриат

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.	ОПК-1;	Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	Темы 1-8		ОПК-1.2.1 умеет классифицировать и оценивать угрозы информационной безопасности.	ОПК-1.1.1 знает понятия информации и информационной безопасности ОПК-1.1.2 знает место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики
2.	ОПК-6;	Способен при решении задач профессиональной деятельности организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;	Темы 1-8		ОПК-6.2.1 умеет разрабатывать модели угроз и модели нарушителя объекта информатизации	ОПК-6.1.5 знает основные угрозы безопасности информации и модели нарушителя объекта информатизации
3.	ДОПК-1	Способен применять математические модели и	Темы 1-8	ДОПК-1.17 владеет навыками применения	ДОПК-1.8 умеет классифицировать	ДОПК-1.2 знает технологии проектирования и построения

		решать задачи помехоустойчивого кодирования при проектировании защищенных телекоммуникационных систем		современных программно-аппаратных средств моделирования информационных процессов и систем ЗИ ДОПК-1.18 владеет навыками оценки адекватности моделей и анализа результатов моделирования	информационные системы по назначению, структуре, типу	информационных систем
4.	ДОПК-2	Способен применять технологии защиты информации при создании защищенных телекоммуникационных систем	Темы 1-8	ДОПК-2.11 владеет навыками классификации информационных систем и средств вычислительной техники по требованиям регуляторов ИБ	ДОПК-2.7 умеет анализировать эффективность применения мер по обеспечению ЗИ и разрабатывать предложения по совершенствованию структуры мер и повышению эффективности	ДОПК-2.1 знает подходы к построению подсистем фиксации и реагирования на инциденты информационной безопасности
5.	ДОПК-3	Способен осуществлять эксплуатацию и проводить техническое обслуживание защищенных телекоммуникационных систем	Темы 1-8	ДОПК-3.12 владеет навыками проведения лицензирования в области защиты информации	ДОПК-3.9 умеет организовывать проведение и сопровождать аттестацию объекта информатизации в соответствии с требованиями нормативных документов	ДОПК-3.1 знает государственные нормативные документы в области организации проведения и сопровождения аттестации объекта информатизации
6.	ДОПК-4	Способен проводить мониторинг функционирования защищенных телекоммуникационных систем	Темы 1-8	ДОПК-4.16 владеет навыками проведения аудита ИБ со сбором данных	ДОПК-4.10 умеет применять инструментальные средства мониторинга и аудита безопасности	ДОПК-4.1 знает стандарты и критерии в области аудита ИБ

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
ОПК-1 ОПК-6 ДОПК-1 ДОПК-2 ДОПК-3 ДОПК-4	Контрольная работа	А) полностью сформирована (компетенция освоена на высоком уровне) – 5 баллов Б) частично сформирована: •компетенция освоена на продвинутом уровне – 4 балла; •компетенция освоена на базовом уровне – 3 балла; В) не сформирована (компетенция не освоена) – 2 и менее баллов	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. Общая характеристика принципов, методов и механизмов обеспечения компьютерной безопасности. Основы обеспечения безопасности информации в компьютерных системах.

2. Исследование объекта защиты информации и анализ его защищённости по видам угроз, классам каналов несанкционированного получения информации, причинам нарушения целостности информации и потенциально возможным злоумышленным действиям.

3. Проектирование архитектуры системы защиты информации выбранного объекта и оценка его уровня защищённости.

4. Виды и анализ угроз автоматизированных систем, компьютерные вирусы, технология и способы вторжения в устойчивую работу автоматизированных систем злоумышленников.

5. Совершенствование системы защиты информации предприятия (фирмы) на основе комплексного применения современных средств защиты информации.

6. Разработка и обоснование требований к системе защиты информации предприятия (фирмы) и рекомендаций по её эффективному наращиванию.

7. Направления повышения эффективности существующей системы защиты и методика применения средств защиты информации на выбранных объектах исследования.

8. Разработка проекта создания системы защиты информации на выбранных типовых офисных объектах.

9. Основные виды атак на компьютерные системы (КС), их классификация, проблемы обеспечения информационной безопасности в проводных КС.

10. Беспроводной доступ к локальным сетям. Угрозы и уязвимости в беспроводных компьютерных системах.

3.2 Примерная тематика контрольной работы:

1. Компьютерная преступность в экономических областях.
2. Компьютерные вирусы в современных информационных системах.
3. Информационные угрозы современным экономическим объектам.
4. Безопасность информации в коммерческой деятельности.
5. Становление и развитие промышленного шпионажа.
6. Модель распространения прав доступа Take-Grant. Цель использования модели Take-Grant. Основные элементы модели Take-Grant. Формальное описание модели Take-Grant.
7. Описание систем защиты с помощью матрицы доступа. Таблицы, описывающие права доступа субъектов к объектам. Описание модели Харрисона-Руззо-Ульмана (HRU).

8. Направления повышения эффективности существующей системы защиты и методика применения средств защиты информации на выбранных объектах исследования.

9. Общий подход к построению систем, реализующих мандатную (полномочную) политику безопасности в модели BL (Белла-Лападулы).

10. Назначение модели Белла-Лападулы. Описание модели Белла-Лападулы (BL). Основная теорема безопасности модели Белла-Лападулы.

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

Формой контроля знаний по дисциплине «Методы и средства защиты информации в компьютерных сетях» являются две текущие аттестации в виде тестов и итоговая аттестация в виде зачета.

Неделя текущего контроля	Вид оценочного средства	Код компетенций, оценивающий знания, умения, навыки	Содержание оценочного средства	Требования к выполнению	Срок сдачи (неделя семестра)	Критерии оценки по содержанию и качеству с указанием баллов
Согласно графика учебного процесса	тестирование	ОПК-1 ОПК-6 ДОПК-1 ДОПК-2 ДОПК-3 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 графика учебного процесса	тестирование	ОПК-1 ОПК-6 ДОПК-1 ДОПК-2 ДОПК-3 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 графика учебного процес	Зачет	ОПК-1 ОПК-6 ДОПК-1 ДОПК-2 ДОПК-3 ДОПК-4	2 вопроса	Зачет проводится в устной форме, путем ответа на вопросы. Время, отведенное на	Результаты предоставляются в день проведения зачета	Критерии оценки: «Зачтено»: - знание основных понятий предмета; - умение использовать и применять полученные

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
са				процедуру – 20 минут на каждого студента		знания на практике; - работа на практических занятиях; - знание основных научных теорий, изучаемых предметов; - ответ на вопросы билета. «Не зачтено»: 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. Функции КСЗИ:
   создание механизмов защиты, сводящие до минимума возможность воздействия дестабилизирующих факторов на защищаемую информацию; непрерывное и оптимальное управление механизмами комплексной защиты
   обеспечение конфиденциальности, целостности, доступности информации
   обеспечение криптографической, программной и аппаратной защиты информации
   обеспечение защиты людей, материальных носителей, автоматизированных систем
2. Требование безопасности повторного использования объектов противоречит:
   инкапсуляции

наследованию
полиморфизму

3. Уровни модели OSI, по возрастанию:
физический, канальный, сетевой, транспортный, сеансовый, представления, прикладной
сетевой, канальный, транспортный, сеансовый, прикладной, представления, физический
прикладной, представления, физический, канальный, сетевой, транспортный, сеансовый
физический, сетевой, канальный, транспортный, сеансовый, представления, прикладной

4. Предположим, что при разграничении доступа учитывается семантика программ. В таком случае на игровую программу могут быть наложены следующие ограничения:
запрет на чтение каких-либо файлов, кроме конфигурационных
запрет на изменение каких-либо файлов, кроме конфигурационных
запрет на установление сетевых соединений

5. Уровни модели TCP/IP, по возрастанию:
канальный, сетевой, транспортный, прикладной
транспортный, канальный, сетевой, прикладной
канальный, транспортный, сетевой, прикладной
прикладной, сетевой, транспортный, канальный

6. К какому уровню модели TCP\IP относятся следующие протоколы HTTP, RTP, FTP, DNS:
прикладной
транспортный
сетевой
канальный

7. В число граней, позволяющих структурировать средства достижения информационной безопасности, входят:
меры обеспечения целостности
административные меры
меры административного воздействия

8. Что входит в функции систем мониторинга:
выявление состояния систем
установка отношений между объектами
установка соответствия правил и обязанностей
все варианты верны

9. Какие существуют подходы по построению защищенных операционных систем применяемых в АС:
фрагментарный и комплексный
фрагментарный и операционный.

комплексный и позиционный.
системный и позиционный.

10. Дублирование сообщений является угрозой:
доступности
конфиденциальности
целостности

11. Какие существуют методы оценки качества КСИБ:
метод оценки уязвимости Хоффмана
экспертная оценка
сигнатурный метод
качественный метод.

12. Самыми опасными источниками внутренних угроз являются:
некомпетентные руководители
обиженные сотрудники
любопытные администраторы

13. Для внедрения бомб чаще всего используются ошибки типа:
отсутствие проверок кодов возврата
переполнение буфера
нарушение целостности транзакций

14. В число целей политики безопасности верхнего уровня входят:
решение сформировать или пересмотреть комплексную программу безопасности
обеспечение базы для соблюдения законов и правил
обеспечение конфиденциальности почтовых сообщений

15. В число целей программы безопасности верхнего уровня входят:
управление рисками
определение ответственных за информационные сервисы
определение мер наказания за нарушения политики безопасности

16. Что означает обеспечение целостности баз данных.

это соответствие информации базы данных её внутренней логике, структуре и заданным правилам.
это полное значение информации базы данных в котором действуют установленные правила
это информация, работающая по установленной структуре базы данных.
это логическая операция обеспечивающая полноту информации и соблюдающая условия того, что информация не будет изменена.

17. В рамках программы безопасности нижнего уровня осуществляются:
стратегическое планирование

повседневное администрирование
отслеживание слабых мест защиты

18. Политика безопасности строится на основе:
общих представлений об ИС организации
изучения политик родственных организаций
анализа рисков

19. В число целей политики безопасности верхнего уровня входят:
формулировка административных решений по важнейшим аспектам реализации программы безопасности
выбор методов аутентификации пользователей
обеспечение базы для соблюдения законов и правил

20. Основные механизмы защиты применяемые в ОС:
идентификации / аутентификации
разграничения доступа
аудита
все перечисленные варианты верны

4.2 Типовые вопросы, выносимые на зачет

1. Общая характеристика принципов, методов и механизмов обеспечения компьютерной безопасности.
2. Структура информационных ресурсов и администрирование в компьютерных системах.
3. Проблемы безопасности компьютерных систем (сетей), понятие угрозы, цели злоумышленников, осуществляющих основные атаки.
4. Виды и анализ угроз автоматизированных систем, компьютерные вирусы, технология и способы вторжения в устойчивую работу автоматизированных систем злоумышленников
5. Уязвимости автоматизированных систем (АС), возможные атаки на них. Особенности построения систем обнаружения атак (СОА) в АС.
6. Угрозы конфиденциальности, целостности, доступности информации, раскрытия параметров информационной системы.
7. Факторы, воздействующие на защищаемую информацию. Классификация угроз. Естественные и искусственные угрозы. Основные направления и методы реализации угроз.
8. Основные виды атак на КС, их классификация. Проблемы обеспечения информационной безопасности в проводных КС.
9. Беспроводной доступ к локальным сетям. Угрозы и уязвимости в беспроводных компьютерных системах.

10. Основные уровни защиты информации в компьютерных системах, организация системы безопасности по уровням компьютерных систем, уровни защиты, в соответствии с механизмами реагирования на угрозы.
11. Машинные носители информации (МНИ), защита МНИ, защита средств взаимодействия с МНИ.
12. Методы и средства обеспечения защиты информации в компьютерных системах, защита представления информации, защита содержания информации.
13. Представьте обобщенную модель защиты объекта, содержащего локальную вычислительную сеть, с безопасной обработкой информации.
14. Какие стадии включает жизненный цикл системы защиты информации (СЗИ), если СЗИ рассматривать как сложную техническую систему? Охарактеризуйте какие процессы включает каждая из стадий.
15. Какие объекты информатизации, инженерные, технические и программно-аппаратные способы и средства могут быть использованы для защиты информации в коммерческих структурах?
16. Перечислите рекомендуемые СТР-К стадии создания системы защиты информации (СЗИ). Какие вопросы решаются на предпроектной стадии, кем она выполняется и чем заканчивается.
17. Сертификация программных и программно-технических средств защиты конфиденциальной компьютерной информации.
18. Методы обеспечения защиты информации – препятствие, маскировка, управление доступом. Функции защиты при управлении доступом. Принуждение и побуждение.
19. Физические средства защиты компьютерных систем. Нейтрализация утечки информации по электромагнитным каналам – применение генераторов шума. Защита от наводок.
20. Аксиомы и определения доступа субъектов к объектам. Понятие объекта относительно языка L. Объекты, входящие в состав компьютерных систем.
21. Аксиома доступа субъектов к объектам. Определение понятия разграничения доступа. Методы разграничения доступа.
22. Дискреционное разграничение доступа. Матрицы доступа. Списки полномочий.
23. Полномочное (мандатное) разграничение доступа. Разграничение по уровням секретности. Различие между дискреционным и мандатным разграничением доступа.
24. Концепция монитора безопасности обращений в компьютерную систему. Правила разграничения доступа субъектов к объектам в ОС.

25. Монитор безопасности обращений (МБО) субъектов к объектам. Схема монитора безопасности обращений. Функции МБО. Свойства МБО.
26. Описание систем защиты с помощью матрицы доступа. Таблицы, описывающие права доступа субъектов к объектам. Описание модели Харрисона-Руззо-Ульмана.
27. Формальное описание системы в модели Харрисона-Руззо-Ульмана. Поведение системы во времени. Понятие монооперационной системы.
28. Теорема о существовании алгоритма определения исходного состояния системы. Условие использования классической модели Харрисона-Руззо-Ульмана. Разрешимость проблемы безопасности.
29. Модель распространения прав доступа Take-Grant. Цель использования модели Take-Grant. Основные элементы модели Take-Grant. Формальное описание модели Take-Grant.
30. Граф доступов. Правила определения переходов системы из состояния в состояние. Условия реализации прав доступа. Расширенная модель Take-Grant, анализ информационных каналов.
31. Пути и стоимости возникновения информационных потоков в расширенной модели Take-Grant.
32. Общий подход к построению систем, реализующих мандатную (полномочную) политику безопасности в модели BL (Белла-Лападулы).
33. Назначение модели Белла-Лападулы. Описание модели Белла-Лападулы (BL). Основная теорема безопасности модели Белла-Лападулы.
34. Условие определения безопасности системы. Свойства безопасности системы. Проверка безопасности системы. Основные теоремы и определения состояний системы.
35. Эквивалентные подходы к определению безопасности модели Белла-Лападулы. Недостатки модели Белла-Лападулы.
36. Структура документации системы менеджмента информационной безопасности в организации. Модель PDCA.
37. Алгоритм и матрица оценки рисков при обеспечении информационной безопасности в организации. Варианты обработки рисков.
38. Требования, предъявляемые к формированию политики безопасности организации. Структура и содержание политики безопасности организации применительно к компьютерным системам.
39. Реализация политики безопасности в компьютерных системах (КС) с использованием механизмов и средств операционных систем. Управление доступом в КС с использованием механизмов и средств сетевых операционных систем.

40. Управление инцидентами информационной безопасности в компьютерных системах.
41. Построение систем защиты от угрозы нарушения конфиденциальности, целостности и доступности компьютерной информации.
42. Фрагментарный и комплексный подходы к созданию систем защиты. Основные достоинства и недостатки фрагментарного подхода. Организация защищенной среды обработки информации при комплексном подходе. Недостатки комплексного подхода.
43. Построение систем защиты от угрозы нарушения конфиденциальности информации. Модель системы защиты от угроз нарушения конфиденциальности информации. Структура системы защиты от угроз нарушения конфиденциальности информации.
44. Построение систем защиты от угрозы нарушения целостности информации. Две основные группы организационно-технологических мер защиты целостности информации. Технологические меры контроля целостности битовых последовательностей, хранящихся на машинных носителях.
45. Построение системы защиты от угрозы нарушения доступности информации. Понятие доступности информации. Основные угрозы доступности информации. Причины возникновения угроз доступности информации. Основные средства защиты от угрозы нарушения доступности информации.
47. Особенности построения парольных систем аутентификации. Парольная защита. Понятия идентификатора и пароля пользователя. Учетная запись пользователя как совокупность его идентификатора и его пароля. Парольная система и состав её элементов.
48. Основные угрозы безопасности парольных систем. Способы получения пароля злоумышленником. Рекомендации по практической реализации парольных систем. Оценка стойкости парольных систем. Методы хранения и передачи паролей. Механизмы хранения паролей в КС.
49. Проблема организации совместного доступа различных приложений к некоторым областям памяти. Основные способы защиты памяти. Барьерные адреса. Механизм функционирования барьерного способа защиты памяти. Способы задания барьерного адреса. Динамические области памяти. Защита данных приложений.
50. Адресные регистры. Особенности способов защиты памяти. Ключ доступа. Организация совместного использования областей памяти. Механизм страничной организации памяти и сегментации.

51. Цифровая подпись. Проблема аутентификации данных или цифровой подписи. Модель аутентификации сообщений. Сравнительный анализ обычной и цифровой подписи.
52. Сущность построения системы защиты информации. Оптимальные механизмы обеспечения защиты информации и механизмы управления. Выбор способа постановки задачи. Методы построения защищённых АС.
53. Что означает термин «аттестация объекта информатизации», раскройте это понятие, какие процедуры предусматриваются для аттестации автоматизированной системы?
54. Этапы разработки защищённой АС. Процесс создания автоматизированных систем в защищенном исполнении (ГОСТ Р 51583—2014). Цель создания автоматизированных систем в защищенном исполнении.
55. Понятие стандарта в области информационной безопасности (ИБ). Обоснование необходимости использования стандартов в области ИБ. Главная задача стандартов в области ИБ.
56. Классификация СВТ по уровню защищённости от НСД к информации. Перечень показателей защищённости СВТ и совокупности описывающих их требований. Характеристика классов защищённости СВТ от НСД к информации.
57. Классификация АС, подлежащих защите от НСД к информации. Требования по защите информации в АС различных классов. Этапы классификации АС. Исходные данные для классификации АС. Выбор класса защищённости АС.

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)

Б1.О.13.04 «Защита информации в ТКС»
(Приложение 2 к рабочей программе)

Направление: 10.03.01 Информационная безопасность

Профиль: Безопасность телекоммуникационных систем (в аэрокосмической сфере)

Уровень высшего образования: бакалавриат

Форма обучения: очная

Королев
2022

1. Общие положения

Цель дисциплины:

Целью изучения дисциплины является формирование у обучаемых специализированной базы знаний по фундаментальным проблемам информационной безопасности в условиях становления современного информационного общества, а также получение навыков в применении технологий обеспечения информационной безопасности объектов регионального уровня, а также в процессе управления информационной безопасностью защищаемых объектов.

Основными **задачами** дисциплины являются:

- ознакомление обучаемых с процессами анализа фундаментальных и прикладных проблем информационной безопасности в условиях становления современного информационного общества, разработка планов и программ проведения научных исследований и технических проектов, подготовка отдельных заданий для исполнителей и выполнение научных исследований по выбранной теме;
- формирование у обучаемых способности самостоятельно организовывать работу коллектива исполнителей, принятию управленческих решений в условиях спектра мнений, определению порядка выполнения работ;
- участие в работах по созданию, изготовлению, монтажу, наладке, испытаниях и сдаче в эксплуатацию систем и средств обеспечения информационной безопасности, разработке проектов методических и нормативных документов, предложений и мероприятий по реализации разработанных проектов и программ;
- формирование обучаемыми предложений по совершенствованию, модернизации, унификации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами.

2. Указания по проведению практических занятий

Тема 1. Введение. Основные понятия теории компьютерной безопасности

Практическое занятие 1

Тема и содержание практического занятия: Актуальность проблемы обеспечения информационной безопасности (ИБ) в компьютерных системах. Современная постановка целей и задач по обеспечению компьютерной

безопасности (переход к тотальной защите и интенсивным мерам). Основные термины и определения в области ИБ компьютерных систем и сетей.

Цель работы: Получить практические знания и навыки о классификации компьютерных систем, подлежащих защите в зависимости от обрабатываемой информации и по функциональному назначению, а также знания о проблематике обеспечения компьютерной безопасности.

Учебные вопросы:

- Современная постановка целей и задач по обеспечению компьютерной безопасности (переход к тотальной защите и интенсивным мерам).
- Основные термины и определения в области ИБ компьютерных систем и сетей.
- Классификация компьютерных систем, подлежащих защите в зависимости от обрабатываемой информации и функционального назначения.
- Общая характеристика принципов, методов и механизмов обеспечения компьютерной безопасности.
- Факты, свидетельствующие о способах злоупотребления информацией, циркулирующей в компьютерных системах.

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

Образовательные технологии: технология формирования ключевых компетентностей.

Продолжительность занятия– 4 ч.

Тема 2. Анализ угроз информационной безопасности для компьютерных систем

Практическое занятие 2

Тема и содержание практического занятия: Виды и анализ угроз автоматизированных систем, компьютерные вирусы, технология и способы вторжения в устойчивую работу автоматизированных систем злоумышленников. Уязвимости АС, возможные атаки на них. Особенности построения систем обнаружения атак (СОА) в АС. Фундаментальные угрозы – утечка информации, нарушение целостности, отказ в обслуживании, незаконное использование. Первичные угрозы – проникновение (маскарад, обход защиты, нарушение полномочий) и внедрение (троянские программы, потайные ходы).

Цель работы: Получить практические знания и навыки об угрозах и возможных атаках, которым могут быть подвергнуты информационные системы.

Учебные вопросы:

- Виды и анализ угроз автоматизированных систем, компьютерные вирусы, технология и способы вторжения в устойчивую работу автоматизированных систем злоумышленников.
- Уязвимости АС, возможные атаки на них.
- Особенности построения систем обнаружения атак (СОА) в АС.
- Угрозы конфиденциальности, целостности, доступности информации, раскрытия параметров информационной системы.
- Причины возникновения угроз безопасности информации. Отличительные особенности угроз корпоративным и локально-вычислительным сетям.

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

Образовательные технологии: технология формирования ключевых компетентностей.

Продолжительность занятия– 4 ч.

Тема 3. Основные уровни защиты информации в компьютерных системах

Практическое занятие 3

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки об уровнях защиты информации в компьютерных системах.

Учебные вопросы:

- Организация системы безопасности по уровням компьютерных систем (КС). Уровни защиты, в соответствии с механизмами реагирования на угрозы.
- Способы защиты данных на различных уровнях. Организация системы безопасности по уровням.
- Машинные носители информации (МНИ). Защита МНИ. Защита средств взаимодействия с МНИ.
- Основные особенности компьютерной информации с точки зрения доступа к ней злоумышленников.
- Виды защищаемой компьютерной информации.
- Условия доступа к защищаемой информации со стороны злоумышленников.

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

Образовательные технологии: технология формирования ключевых компетентностей.

Продолжительность занятия– 4 ч.

Тема 4. Основные положения формальной теории защиты информации

Практическое занятие 4

Тема и содержание практического занятия: Аксиомы и определения доступа субъектов к объектам. Понятие объекта относительно языка L. Объекты, входящие в состав КС. Язык описания клавиатуры. Преобразование. Пример преобразования. Инициирование действия преобразования. Два состояния преобразования. Понятие домена. Процесс. Определение субъекта. Виды доступа к субъекту. Информационный поток. Запись.

Цель работы: Получить практические знания и навыки по методам разграничения доступа в информационных системах.

Учебные вопросы:

- Аксиома доступа субъектов к объектам.
- Определение понятия разграничения доступа. Методы разграничения доступа.
- Дискреционное разграничение доступа. Матрицы доступа. Списки полномочий.
- Полномочное (мандатное) разграничение доступа. Разграничение по уровням секретности.
- Различие между дискреционным и мандатным разграничением доступа.
- Ролевое разграничение доступа.

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

Образовательные технологии: технология формирования ключевых компетентностей.

Продолжительность занятия– 4 ч.

Тема № 5. Формальные модели безопасности

Практическое занятие 5

Тема и содержание практического занятия: Описание систем защиты с помощью матрицы доступа. Таблицы, описывающие права доступа субъектов к объектам. Описание модели Харрисона-Руззо-Ульмана (HRU).

Модель распространения прав доступа Take-Grant. Цель использования модели Take-Grant. Основные элементы модели Take-Grant. Формальное описание модели Take-Grant.

Цель работы: получить практические знания и навыки об основных формальных логических моделях доступа.

Учебные вопросы:

- Описание систем защиты с помощью матрицы доступа. Таблицы, описывающие права доступа субъектов к объектам. Описание модели Харрисона-Руззо-Ульмана (HRU).
- Моделирование поведения системы во времени. Основные команды и операции, моделирующие поведение системы. Примеры команд, используемых при переходе системы из одного состояния в другое.
- Формальное описание системы в модели HRU. Поведение системы во времени.
- Понятие монооперационной системы. Теорема о существовании алгоритма определения исходного состояния системы. Условие использования классической модели HRU. Разрешимость проблемы безопасности.
- Модель распространения прав доступа Take-Grant. Цель использования модели Take-Grant.
- Основные элементы модели Take-Grant. Формальное описание модели Take-Grant.
- Граф доступов. Правила определения переходов системы из состояния в состояние. Условия реализации прав доступа.
- Расширенная модель Take-Grant, анализ информационных каналов.
- Пути и стоимости возникновения информационных потоков в расширенной модели Take-Grant.

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

Образовательные технологии: технология формирования ключевых компетентностей.

Продолжительность занятия– 4 ч.

Тема № 6. Концептуальные положения системы менеджмента информационной безопасности применительно к компьютерным системам

Практическое занятие 6

Тема и содержание практического занятия: Структура документации системы менеджмента информационной безопасности в организации. Модель PDCA. Алгоритм и матрица оценки рисков при обеспечении информационной безопасности в организации. Варианты обработки рисков.

Требования, предъявляемые к формированию политики безопасности организации. Структура и содержание политики безопасности организации применительно к компьютерным системам.

Цель работы: получить практические знания и навыки об управлении информационной безопасностью и формированию политики информационной безопасности в организации.

Учебные вопросы:

- Структура документации системы менеджмента информационной безопасности в организации. Модель PDCA.
- Алгоритм и матрица оценки рисков при обеспечении информационной безопасности в организации. Варианты обработки рисков.
- Требования, предъявляемые к формированию политики безопасности организации.
- Структура и содержание политики безопасности организации применительно к компьютерным системам.
- Цель работы: получить практические знания и навыки об управлении информационной безопасностью и формированию политики информационной безопасности в организации.

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

Образовательные технологии: технология формирования ключевых компетентностей.

Продолжительность занятия– 4 ч.

Тема № 7. Построение систем защиты от угрозы нарушения конфиденциальности, целостности и доступности компьютерной информации

Практическое занятие 7

Тема и содержание практического занятия: Фрагментарный и комплексный подходы к созданию систем защиты. Основные достоинства и недостатки фрагментарного подхода. Организация защищенной среды обработки информации при комплексном подходе. Построение систем защиты от угрозы нарушения конфиденциальности, целостности и доступности компьютерной информации.

Цель работы: получить практические знания и навыки по построению систем защиты от угрозы нарушения конфиденциальности, целостности и доступности компьютерной информации.

Учебные вопросы:

• Фрагментарный и комплексный подходы к созданию систем защиты. Основные достоинства и недостатки фрагментарного подхода.

• Организация защищенной среды обработки информации при комплексном подходе. Недостатки комплексного подхода. Условия эффективной работы средств защиты информации.

• Организация защиты субъектов информационных отношений.

• Построение систем защиты от угрозы нарушения конфиденциальности, целостности и доступности компьютерной информации.

• Построение систем защиты от угрозы нарушения конфиденциальности информации. Модель системы защиты от угроз нарушения конфиденциальности информации. Структура системы защиты от угроз нарушения конфиденциальности информации.

• Построение систем защиты от угрозы нарушения целостности информации. Две основные группы организационно-технологических мер защиты целостности информации.

• Технологические меры контроля целостности битовых последовательностей, хранящихся на машинных носителях.

• Циклический контрольный код как механизм обеспечения контроля целостности информации.

• Интегрированный подход для обеспечения целостности данных. Основные принципы обеспечения целостности данных. Обеспечение защиты целостности программно-аппаратной среды.

• Построение системы защиты от угрозы нарушения доступности информации. Понятие доступности информации.

• Основные угрозы доступности информации. Причины возникновения угроз доступности информации.

• Основные средства защиты от угрозы нарушения доступности информации.

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

Образовательные технологии: технология формирования ключевых компетентностей.

Продолжительность занятия– 2 ч.

Тема № 8. Методология обследования и проектирования защищенных информационных (автоматизированных) систем
Практическое занятие 8

Тема и содержание практического занятия: Сущность построения системы защиты информации. Оптимальные механизмы обеспечения защиты информации и механизмы управления. Выбор способа постановки задачи. Методы построения защищённых АС. Принципы проектирования. Структурный принцип и принцип модульного проектирования. Три

основных конструкции для проектирования. Преимущества использования модульного принципа.

Корректность реализации и верификация информационных (автоматизированных) систем. Понятие корректности или правильности проверяемого объекта. Спецификация требований программного обеспечения.

Представления функциональных требований. Рекомендации к структуре и методам описания программных требований. Основные ключевые требования «хорошей спецификации». Требования к программной спецификации. Основные подходы к определению спецификаций требований.

Теория безопасных систем (ТСВ). Понятие «доверенная вычислительная среда» (trusted computing base-TCB). Дискретная природа характеристики «безопасный». Характеристика «доверенный». Доверенная вычислительная среда. Набор компонентов, составляющий доверенную вычислительную среду. Этапы разработки защищённой АС. Процесс создания автоматизированных систем в защищенном исполнении (ГОСТ Р 51583—2000). Цель создания АСЗИ.

Цель работы: получить практические знания и навыки об этапах и содержании работ по проектированию защищенных информационных (автоматизированных) систем.

Учебные вопросы:

- Сущность построения системы защиты информации. Оптимальные механизмы обеспечения защиты информации и механизмы управления. Выбор способа постановки задачи.
- Методы построения защищённых АС. Два основных метода проектирования. Метод проектирования «снизу вверх». Недостатки метода проектирования «снизу вверх».
- Иерархический метод построения защищённой АС («сверху вниз»).
- Принципы проектирования. Структурный принцип и принцип модульного проектирования.
- Три основных конструкции для проектирования. Использование элемента DO-WHILE для организации цикла. Конструкция принятия двоичного решения IF-THEN-ELSE. Преимущества использования модульного принципа.
- Корректность реализации и верификация информационных (автоматизированных) систем. Понятие корректности или правильности проверяемого объекта.
- Спецификация требований программного обеспечения. Функциональные критерии и характеристики. Неформализованные представления разработчика. Спецификация требований программного обеспечения (Software Requirements Specification).
- Представления функциональных требований. Рекомендации к структуре и методам описания программных требований. Основные ключевые требования «хорошей спецификации». Требования к программной

спецификации. Основные подходы к определению спецификаций требований.

- Теория безопасных систем (ТСВ). Понятие «доверенная вычислительная среда» (trusted computing base-TCB).
- Дискретная природа характеристики «безопасный». Характеристика «доверенный». Доверенная вычислительная среда. Набор компонентов, составляющий доверенную вычислительную среду.
- Этапы разработки защищённой автоматизированной системы (АСЗИ). Процесс создания автоматизированных систем в защищенном исполнении (ГОСТ Р 51583—2014). Цель создания АСЗИ.

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

Образовательные технологии: технология формирования ключевых компетентностей.

Продолжительность занятия– 2 ч.

Тема № 9. Общие сведения о стандартах в области информационной безопасности
Практическое занятие 9

Тема и содержание практического занятия: Понятие стандарта в области информационной безопасности (ИБ). Обоснование необходимости использования стандартов в области ИБ. Главная задача стандартов в области ИБ. Стандарты как основной механизм обеспечения совместимости продуктов и систем.

Классификация СВТ по уровню защищённости от НСД к информации. Перечень показателей защищённости СВТ и совокупности описывающих их требований. Характеристика классов защищённости СВТ от НСД к информации.

Классификация АС, подлежащих защите от НСД к информации. Требования по защите информации в АС различных классов. Этапы классификации АС. Исходные данные для классификации АС. Выбор класса защищённости АС.

Аудит. Идентификация и аутентификация. Механизм защиты данных. Регистрация и учёт. Корректность. Контроль корректности функционирования средств защиты. Непрерывность защиты.

Основные положения «Общих критериев». Свойство «Общих критериев». Структура «Общих критериев». Определение объекта оценки и продукта. Система как специфическое воплощение ИТ с конкретным назначением и условиями эксплуатации.

Профили защиты. Введение профиля защиты. Идентификация профиля защиты. Аннотация профиля защиты. Описание объекта оценки. Характерные особенности ИТ применительно к объекту оценки (ОО).

Среда безопасности ОО. Описание аспектов безопасности среды, в которой предполагается использовать ОО. Структура и содержание профиля защиты. Цели безопасности для ОО. Цели безопасности для среды ОО.

Функциональные требования и требования доверия. Основные осуществляемые операции при выборе компонентов функциональных требований. Требования доверия к безопасности ОО. Обоснование профиля защиты.

Цель работы: получить практические знания и навыки о применении стандартов в области информационной безопасности

Учебные вопросы:

- Понятие стандарта в области информационной безопасности (ИБ). Обоснование необходимости использования стандартов в области ИБ. Главная задача стандартов в области ИБ. Стандарты как основной механизм обеспечения совместимости продуктов и систем.
- Основы взаимодействия между производителями, потребителями и экспертами по квалификации продуктов информационных технологий (ИТ). Регламентация необходимости применения средств, механизмов, алгоритмов. Требования безопасности.
- Классификация СВТ по уровню защищённости от НСД к информации. Перечень показателей защищённости СВТ и совокупности описывающих их требований. Характеристика классов защищённости СВТ от НСД к информации.
- Классификация АС, подлежащих защите от НСД к информации. Требования по защите информации в АС различных классов. Этапы классификации АС. Исходные данные для классификации АС. Выбор класса защищённости АС.
- Набор требований к подсистемам защиты АС. Проверка соответствия требованиям по защите информации от НСД для АС. Показатели защищённости от НСД к информации в АС.
- Стандарт «Критерии оценки доверенных компьютерных систем»/ TCSEC («Оранжевая книга»). Цель разработки стандарта TCSEC. Требования безопасности, предъявляемых к аппаратному, программному и специальному обеспечению компьютерных систем. Категории требований безопасности. Общая структура требований к системам защиты.
- Политика безопасности. Возможность осуществления субъектами доступа к объектам. Разграничение доступа к категорированной информации. Метки безопасности как механизм контроля доступа.
- Аудит. Идентификация и аутентификация. Механизм защиты данных. Регистрация и учёт. Корректность. Контроль корректности функционирования средств защиты. Непрерывность защиты.
- Основные положения «Общих критериев». Свойство «Общих критериев». Структура «Общих критериев». Определение объекта оценки и продукта. Система как специфическое воплощение ИТ с конкретным назначением и условиями эксплуатации.

- Категории пользователей. Среда безопасности. Задачи, решаемые при подготовке к оценке. Требования по безопасности. Каталоги требований безопасности. Общая модель безопасности. Недостатки «Общих критериев».
- Профили защиты. Введение профиля защиты. Идентификация профиля защиты. Аннотация профиля защиты. Описание объекта оценки. Характерные особенности ИТ применительно к объекту оценки (ОО).
- Среда безопасности ОО. Описание аспектов безопасности среды, в которой предполагается использовать ОО. Структура и содержание профиля защиты. Цели безопасности для ОО. Цели безопасности для среды ОО.
- Функциональные требования и требования доверия. Основные осуществляемые операции при выборе компонентов функциональных требований. Требования доверия к безопасности ОО. Обоснование профиля защиты.

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

Образовательные технологии: технология формирования ключевых компетентностей.

Продолжительность занятия– 2 ч.

Тема № 10. Концепция защиты СВТ и АС от НСД в соответствии с руководящими документами Гостехкомиссии и нормативно-методическими документами ФСТЭК России

Практическое занятие 10

Тема и содержание практического занятия: Перечень основных документов ФСТЭК РФ по вопросам защиты информации. Основные положения концепции защиты СВТ и АС от НСД к информации. Принципы защиты от НСД. Построение модели нарушителя безопасности АС. Система разграничения доступа (СРД) и её функции. Средства для СРД. Реализация СРД. Проверка выполнения технических требований по защите. Сертификат соответствия СВТ или АС требованиям по защите.

Цель работы: получить практические знания и навыки по защите СВТ и АС от НСД.

Учебные вопросы:

- Перечень основных документов ФСТЭК РФ по вопросам защиты информации. Основные положения концепции защиты СВТ и АС от НСД к информации.
- Определение НСД к информации. Два направления защиты от НСД. Особенности функций защиты в СВТ и АС. Основные способы НСД. Принципы защиты от НСД.

- Построение модели нарушителя безопасности АС. Уровни возможностей, предоставляемые нарушителям штатными средствами АС и СВТ.
- Характеристики оценки технических средств защиты от НСД. Система разграничения доступа (СРД) и её функции. Средства для СРД.
- Реализация СРД. Проверка выполнения технических требований по защите. Сертификат соответствия СВТ или АС требованиям по защите.

*Вид практического занятия**:** смешанная форма практического занятия.*
Образовательные технологии: технология формирования ключевых компетентностей.
Продолжительность занятия– 2 ч.

3. Указания по проведению лабораторного практикума

Не предусмотрено учебным планом.

4. Указания по проведению самостоятельной работы студентов

Самостоятельная работа студентов (СРС) основана на самостоятельном формировании у учащихся знаний, умений, навыков и компетенций и направлена на реализацию принципов обучения, связанных с саморазвитием личности в процессе обучения, формированием активных методов и технологий познавательной деятельности.

В соответствии с общим объемом часов, отведенных для изучения дисциплины, предусматривается выполнение следующих видов самостоятельных работ студентов (СРС): самостоятельное изучение теоретического материала с самоконтролем по приведенным ниже вопросам, изучение теоретического материала при подготовке к защите лабораторных работ, итоговое повторение теоретического материала при подготовке к экзамену.

При организации самостоятельной работы студентов на преподавателей возлагается управление, включающее планирование работы, консультирование студентов, текущий контроль и анализ результатов учебной работы. При этом планируемый объем СРС занимает большую часть учебной нагрузки студентов университета. Основными видами самостоятельной работы студентов без участия преподавателей при освоении в университете образовательных программ являются: − формирование и изучение содержания конспекта лекций на базе рекомендованной лектором учебной литературы, включая информационные образовательные ресурсы; − написание рефератов;

− подготовка к лабораторным работам, их оформление; − компьютерный текущий самоконтроль и контроль успеваемости на базе электронных обучающих и аттестующих тестов; Основными видами

самостоятельной работы студентов с участием преподавателя для ее управления в учебном процессе являются: − текущие консультации и контроль по формированию и освоению теоретического содержания дисциплин; − прием и защита лабораторных работ; − консультирование и прием рефератов; − консультирование по результатам текущего компьютерного контроля знаний; − прием экзамена по дисциплине.

При написании реферата или подготовке к выполнению домашнего задания в форме доклада следует предварительно изучить соответствующий материал по предлагаемой теме. Для этого можно воспользоваться конспектом лекций, презентацией курса, литературой по заданной теме.

№ п/п	Наименование блока (раздела) дисциплины	Виды СРС
1.	Введение. Основные понятия теории компьютерной безопасности	***Подготовка докладов и презентаций по темам:*** Классификация компьютерных систем, подлежащих защите в зависимости от обрабатываемой информации и функционального назначения. Классификация СВТ по уровню защищённости от НСД к информации. Перечень показателей защищённости СВТ и совокупности описывающих их требований. Характеристика классов защищённости СВТ от НСД к информации. Виды и анализ угроз автоматизированных систем, компьютерные вирусы, технология и способы вторжения в устойчивую работу автоматизированных систем злоумышленников.
2.	Анализ угроз информационной безопасности для компьютерных систем	***Подготовка докладов и презентаций по темам:*** Классификация компьютерных систем, подлежащих защите в зависимости от обрабатываемой информации и функционального назначения. Классификация СВТ по уровню защищённости от НСД к информации. Перечень показателей защищённости СВТ и совокупности описывающих их требований. Характеристика классов защищённости СВТ от НСД к информации. Виды и анализ угроз автоматизированных систем, компьютерные вирусы, технология и способы вторжения в устойчивую работу автоматизированных систем злоумышленников.
3	Основные уровни защиты информации в	***Подготовка докладов и презентаций по темам:***

	компьютерных системах	Классификация АС, подлежащих защите от НСД к информации. Требования по защите информации в АС различных классов. Этапы классификации АС. Исходные данные для классификации АС. Выбор класса защищённости АС. Структура документации системы менеджмента информационной безопасности в организации. Модель PDCA. Алгоритм и матрица оценки рисков при обеспечении информационной безопасности в организации. Варианты обработки рисков.
4	Основные положения формальной теории защиты информации	***Подготовка докладов и презентаций по темам:*** Перечень основных документов ФСТЭК России по вопросам защиты информации. Система разграничения доступа (СРД) и её функции. Средства для СРД. Реализация СРД.
5	Формальные модели безопасности	***Подготовка докладов и презентаций по темам:*** Построение модели нарушителя безопасности АС. Уровни возможностей, предоставляемые нарушителям штатными средствами АС и СВТ. Базовая модель угроз ИСПДн. Модель распространения прав доступа Take-Grant. Цель использования модели Take-Grant. Основные элементы модели Take-Grant. Формальное описание модели Take-Grant.
6	Концептуальные положения системы менеджмента информационной безопасности применительно к компьютерным системам	***Подготовка докладов и презентаций по темам:*** Лицензирование и сертификация в области защиты информации. Комплексные системы защиты информации. Аттестация АС по требованиям безопасности информации.
7	Построение систем защиты от угрозы нарушения конфиденциальности, целостности и доступности компьютерной информации	***Подготовка докладов и презентаций по темам:*** Описание систем защиты с помощью матрицы доступа. Таблицы, описывающие права доступа субъектов к объектам. Описание модели Харрисона-Руззо-Ульмана (HRU). Сущность построения системы защиты информации. Оптимальные механизмы обеспечения защиты информации и механизмы управления. Выбор способа

		постановки задачи. Методы построения защищённых АС. Принципы проектирования. Структурный принцип и принцип модульного проектирования. Три основных конструкции для проектирования. Преимущества использования модульного принципа.

5. Указания по проведению контрольных работ для студентов очной формы обучения

5.1 Требования к структуре.

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

5.2 Требования к содержанию (основной части).

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

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.

Основная часть работы включает 2 - 4 вопроса, каждый из которых посвящается решению задач, сформулированных во введении, и заканчивается констатацией итогов.

Приветствуется иллюстрация содержания работы таблицами, графическим материалом (рисунками, схемами и т.п.).

Необходимо давать ссылки на используемую Вами литературу.

Заключение должно содержать сделанные автором работы выводы, итоги исследования.

Вслед за заключением идет список литературы, который должен быть составлен в соответствии с установленными требованиями. Если в работе имеются приложения, они оформляются на отдельных листах, и должны быть соответственно пронумерованы.

Требования к оформлению.

Объём контрольной работы – 20 страниц формата А 4, напечатанного с одной стороны текста (1,5 интервал, шрифт Times New Roman).

Примерная тематика контрольных работ:

1. Методы и средства обеспечения защиты информации в компьютерных системах, защита представления информации, защита содержания информации.
2. Представьте обобщенную модель защиты объекта, содержащего локальную вычислительную сеть, с безопасной обработкой информации.

3. Какие стадии включает жизненный цикл системы защиты информации (СЗИ), если СЗИ рассматривать как сложную техническую систему? Охарактеризуйте какие процессы включает каждая из стадий.

4. Какие объекты информатизации, инженерные, технические и программно-аппаратные способы и средства могут быть использованы для защиты информации в коммерческих структурах?

5. Перечислите рекомендуемые СТР-К стадии создания системы защиты информации (СЗИ). Какие вопросы решаются на предпроектной стадии, кем она выполняется и чем заканчивается.

6. Сертификация программных и программно-технических средств защиты конфиденциальной компьютерной информации.

7. Методы обеспечения защиты информации – препятствие, маскировка, управление доступом. Функции защиты при управлении доступом. Принуждение и побуждение.

6. Перечень основной и дополнительной учебной литературы

Основная литература:

1. Баранова Е.К., Бабаш А.В. Информационная безопасность и защита информации : учебное пособие. Издательство: РИОР. Год издания: 2022. ISBN: 978-5-369-01761-6

2. Бондарев В.В. Введение в информационную безопасность автоматизированных систем : учебное пособие. Москва : Издательство МГТУ им. Н.Э. Баумана, 2016. ISBN 978-5-7038-4414-4

7.2 Дополнительная литература:

1. Шаньгин В. Ф. Информационная безопасность. - М.: ДМК Пресс, 2014. - 702 с.: ил. ISBN 978-5-94074-768-0
2. Оценка относительного ущерба безопасности информационной системы: Монография / Е.А. Дубинин, Ф.Б. Тебуева, В.В. Копытов. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2014. - 192 с.: ил.; 60x88 1/16 11 с.. - (Научная мысль). (о) ISBN 978-5-369-01371-7.
3. Майкл Коллинз. Защита сетей. Подход на основе анализа данных / пер. с анг. А.В. Добровольская. –М.: ДМК Пресс, 2020. ISBN 978-5-97060-649-0

7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

Интернет-ресурсы:

1. **http://www.gov.ru** - сервер органов государственной власти Российской Федерации.

2. **http://www.minfin.ru** - официальный сайт Министерства финансов Российской Федерации.

3. http://www.biblioclub.ru

4. http://znanium.com

8. Перечень информационных технологий

- **Перечень программного обеспечения:** MSOffice, PowerPoint.

- **Информационные справочные системы:**
  1. Ресурсы информационно-образовательной среды МГОТУ.
  2. Рабочая программа и методическое обеспечение по дисциплине: «Защита информации в ТКС»