МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тверской государственный технический университет»
(ТвГТУ)

УТВЕРЖДАЮ
Проректор
по учебной работе
_____ Э.Ю. Майкова
« _____ » _____ 2020 г.

РАБОЧАЯ ПРОГРАММА

дисциплины части, формируемой участниками образовательных
отношений Блока 1 «Дисциплины (модули)»
«Защита информации в радиоэлектронных системах»

Направление подготовки специалистов – 11.05.01 Радиоэлектронные системы и комплексы.

Направленность (профиль) – Радиолокационные системы и комплексы.

Типы задач профессиональной деятельности: проектный, научно-исследовательский.

Форма обучения – очная.

Факультет информационных технологий
Кафедра «Радиотехнические информационные системы»

Тверь 2020

Рабочая программа дисциплины соответствует ОХОП подготовки специалистов в части требований к результатам обучения по дисциплине и учебному плану.

Разработчик программы: проф. кафедры РИС В.К. Кемайкин

Программа рассмотрена и одобрена на заседании кафедры РИС
«15» мая 2020г., протокол № 6.

Заведующий кафедрой С.Ф. Боев

Согласовано
Начальник учебно-методического
отдела УМУ Д.А. Барчуков

Начальник отдела
комплектования
зональной научной библиотеки О.Ф. Жмыхова

1. Цели и задачи дисциплины

Цели дисциплины:

изучение методов защиты и основных закономерностей передачи информации в цифровых телекоммуникационных системах.

Задачи дисциплины:

формирование у студентов компетенций, позволяющих самостоятельно проводить математический анализ физических процессов в аналоговых и цифровых устройствах формирования, преобразования и обработки сигналов, оценивать реальные и предельные возможности пропускной способности и помехоустойчивости телекоммуникационных систем и сетей.

2. Место дисциплины в структуре ОП

Дисциплина относится к части, формируемой участниками образовательных отношений Блока 1 ОП ВО. Для изучения курса требуются знания, умения и навыки, полученные в процессе изучения дисциплины «Кодирование и шифрование информации в радиоэлектронных системах».

Приобретенные знания в рамках данной дисциплины помимо их самостоятельного значения используются при выполнении выпускной квалификационной работы.

3. Планируемые результаты обучения по дисциплине

3.1 Планируемые результаты обучения по дисциплине

Компетенции, закрепленные за дисциплиной в ОХОП:

ПК-2 Способен решать задачи оптимизации существующих и новых технических решений в условиях априорной неопределенности с применением пакетов прикладных программ.

Индикаторы компетенций, закреплённых за дисциплиной в ОХОП:

ИПК-2.1. Использует методы оптимизации для существующих и новых технических решений в условиях априорной неопределенности.

Показатели оценивания индикаторов достижения компетенций

Знать:

З1.1. методы оптимизации существующих и новых технических решений в условиях априорной неопределенности систем защиты информации в радиоэлектронных системах постановку задачи отождествления данных при траекторной обработке.

Уметь:

У1.1. применять современный математический аппарат для решения задачи оптимизации в радиоэлектронных системах защиты информации

Иметь опыт практической подготовки:

ПП1.1. в применении современных теоретических и экспериментальных методов исследования с целью создания новых перспективных средств инженерной защиты в радиоэлектронных системах;

ПК-3 Способен к реализации программ экспериментальных исследований, в том числе в режиме удаленного доступа, включая выбор технических средств, обработку результатов и оценку погрешности экспериментальных данных.

Индикаторы компетенций, закреплённых за дисциплиной в ОХОП:

ИПК-3.1. Применяет на практике знания принципов планирования экспериментальных исследований.

Показатели оценивания индикаторов достижения компетенций

Знать:

З2.1. методы и способы планирования экспериментальных исследований в области защиты в радиоэлектронных системах;

Уметь:

У2.1. применять современные теоретические и экспериментальные методы исследования с целью создания новых перспективных средств инженернотехнической защиты радиоэлектронных систем; организовывать и проводить их испытания с целью оценки соответствия требованиям технических регламентов, международных и национальных стандартов и иных нормативных документов.

Иметь опыт практической подготовки:

ПП2.1. планирования экспериментальных исследований в области защиты в радиоэлектронных системах;

Индикаторы компетенций, закреплённых за дисциплиной в ОХОП:

ИПК-3.3. Проводит экспериментальные исследования, в том числе в режиме удаленного доступа.

Показатели оценивания индикаторов достижения компетенций

Знать:

З3.1. Сформулировать принципы планирования экспериментальных исследований

Уметь:

У3.1. Обосновывать программу эксперимента, обрабатывать результаты эксперимента, оценивать погрешности экспериментальных данных

Иметь опыт практической подготовки:

ПП3.1. Иметь практический опыт проведения экспериментальных исследований

3.2. Технологии, обеспечивающие формирование компетенций

Проведение лекционных, лабораторных и практических занятий.

4. Трудоемкость дисциплины и виды учебной работы

Таблица 1а. Распределение трудоемкости дисциплины по видам учебной работы

Вид учебной работы	Зачетные единицы	Академические часы
Общая трудоемкость дисциплины	5	180
Аудиторные занятия (всего)		95
В том числе:		
Лекции		38

Практические занятия (ПЗ)		38
Лабораторные работы (ЛР)		19
Самостоятельная работа обучающихся (всего)		49+36 (экз)
В том числе:		
Курсовая работа		не предусмотрены
Курсовой проект		не предусмотрены
Расчетно-графические работы		не предусмотрены
Реферат		не предусмотрены
Другие виды самостоятельной работы: - подготовка к защите лабораторных работ - подготовка к защите практических работ		29
Текущий контроль успеваемости и промежуточная аттестация (экзамен)		20+36 (экз)
Практическая подготовка при реализации дисциплины (всего)		57
Практические занятия (ПЗ)		38
Лабораторные работы (ЛР)		19
Курсовая работа		не предусмотрены
Курсовой проект		не предусмотрены

5. Структура и содержание дисциплины

5.1. Структура дисциплины

Таблица 2. Модули дисциплины, трудоемкость в часах и виды учебной работы

№	Наименование модуля	Труд-ть часы	Лекции	Практич. занятия	Лаб. практикум	Сам. работа
1	Предмет курса. Информационная безопасность в системе национальной безопасности Российской Федерации	13	3	-	-	6+4 (экз)
2	Основные понятия теории информационной безопасности. Анализ угроз информационной безопасности	22	5	7	-	5+5 (экз)
3	Методы и средства обеспечения информационной безопасности в радиоэлектронных системах передачи информации	32	5	8	6	9+4 (экз)
4	Основы комплексного обеспечения информационной безопасности в радиоэлектронных системах передачи	29	3	10	6	5+5 (экз)
5	Стандарты информационной безопасности, критерии и классы оценки защищенности	31	9	9	-	7+6 (экз)
6	Методология построения и	23	8	-	-	9+6 (экз)

	анализа систем обеспечения информационной безопасности					
7	Технические каналы утечки информации в радиоэлектронных системах передачи	30	5	4	7	8+6 (экз)
Всего на дисциплину		**180**	38	38	19	49+36 (экз)

5.2. Содержание дисциплины

МОДУЛЬ 1 «Предмет курса. Информационная безопасность в системе национальной безопасности Российской Федерации»

Цели и задачи курса. Предмет, структура и краткое содержание курса. История возникновения и развития систем защиты информации. Понятие национальной безопасности. Виды безопасности личности, общества и государства: экономическая, внутриполитическая, социальная, международная, информационная, военная, пограничная, экологическая и другие. Виды защищаемой информации. Основные понятия и общеметодологические принципы теории информационной безопасности. Роль информационной безопасности в обеспечении национальной безопасности государства. Обеспечение информационной безопасности в нормальных и чрезвычайных ситуациях. Основные правовые и нормативные акты в области информационной безопасности. Методические указания по изучению курса. Рекомендуемая основная и дополнительная литература.

МОДУЛЬ 2 «Основные понятия теории информационной безопасности. Анализ угроз информационной безопасности»

Основные понятия теории компьютерной безопасности. Понятие информации, ин формационной безопасности АС. Субъектнообъектная модель информационной системы. Основные определения. Язык. Объекты. Субъекты. Доступ. Информационный поток. Монитор безопасности. Ядро безопасности. Иерархические моде ли вычислительных систем и модель взаимодействия открытых систем (OSI/ISO). Ценность информации. Аддитивная модель. Порядковая шкала. Решетка ценности. Анализ угроз информационной безопасности. Угрозы конфиденциальности, целостности, доступности информации, раскрытия параметров информационной системы. Структура теории компьютерной безопасности. Основные уровни защиты информации. Защита машинных носителей информации (МНИ). Защита средств взаимодействия с МНИ. Защита представления информации. Защита содержания информации. Основные виды атак на информационные АС. Классификация основных атак и вредоносных программ.

МОДУЛЬ 3 «Методы и средства обеспечения информационной безопасности в радиоэлектронных системах передачи информации»

Построение систем защиты от угрозы нарушения конфиденциальности информации. Организационно режимные меры. Защита от несанкционированного доступа (НСД). Построение парольных систем. Криптографические методы защиты.

Защита от угрозы нарушения конфиденциальности на уровне содержания информации. Построение систем защиты от угрозы нарушения целостности информации. Организационно-технологические меры защиты. Защита целостности программно-аппаратной среды. Основные методы защиты памяти. Цифровая подпись. Защита от угрозы целостности на уровне содержания информации. Построение системы защиты от угрозы доступности информации. Эксплуатационно-технологические меры защиты. Защита от сбоев программно-аппаратной среды. Защита семантического анализа и актуальности информации. Построение системы защиты от угрозы раскрытия параметров информационной системы. Сокрытие характеристик носителей. Мониторинг использования систем защиты. Защита параметров представления и содержания информации.

МОДУЛЬ 4 «Основы комплексного обеспечения информационной безопасности в радиоэлектронных системах передачи»

Понятие политики безопасности. Политика (стратегия) безопасности. Дискреционная политика разграничения доступа. Мандатная (полномочная) политика разграничения доступа. Разработка и реализация политики безопасности. Модели безопасности. Описание систем защиты с помощью матрицы доступа. Модель Харрисона-Руззо-Ульмана (HRU). Разрешимость проблемы безопасности. Модель распространения прав доступа Take-Grant. Расширенная модель Take-Grant, анализ информационных каналов. Описание модели Белла-Лападулы (BL). Основная теорема безопасности модели Белла-Лападулы. Эквивалентные подходы к определению безопасности модели Белла-Лападулы. Решетка мандатных моделей. Ролевая политика безопасности.

МОДУЛЬ 5 «Стандарты информационной безопасности, критерии и классы оценки защищенности»

Основные критерии защищенности информационных автоматизированных систем (АС). Классы защищенности АС. Критерии и классы защищенности средств вычислительной техники (СВТ), и АС. Стандарты по оценки защищенности АС. Стандарт оценки безопасности компьютерных систем TCSEC («Оранжевая книга»). Основные требования к системам защиты в TCSEC. Классы защиты TCSEC. Концепция защиты АС и СВТ по руководящим документам Гостехкомиссии РФ. Классификация СВТ по документам Гостехкомиссии. Классификация АС по документам Гостехкомиссии, требования классов защиты. Единые критерии безопасности информационных технологий (Common Criteria). Основные положения «Единых критериев». Требования безопасности. Профили защиты.

МОДУЛЬ 6 «Методология построения и анализа систем обеспечения информационной безопасности»

Применение иерархического метода для построения защищенной АС. Исследование корректности реализации и методы верификации АС. Теория безопасных систем (ТСВ). Информационные АС и программные средства, сертифицированные в соответствии с требованиями «Оранжевой книги». Проблемы компьютерной безопасности. Перспективные направления исследований в области

компьютерной безопасности. Центры компьютерной безопасности. Рекомендации по самостоятельному углубленному изучению разделов курса.

МОДУЛЬ 7 «Технические каналы утечки информации в радиоэлектронных системах передачи»

Понятие и особенности утечки информации. Структура, классификация и основные характеристики технических каналов утечки информации. Простые и составные технические каналы утечки информации. Характеристика и возможности оптических, акустических, радиоэлектронных и материально-вещественных каналов утечки информации.

5.3. Лабораторные работы

Таблица 3. Лабораторные работы и их трудоемкость.

Порядковый номер модуля. Цели лабораторных работ	**Наименование лабораторных работ**	**Трудоемкость в часах**
Модуль 3 **Цель:** изучить международный стандарт безопасности информационных систем ISO. Исследовать системы защиты информации «Страж NT», «SecretNet» и «Dallas»	Изучение международного стандарта безопасности информационных систем ISO. Исследование системы защиты информации «Страж NT». Система защиты информации SecretNet. Система защиты информации Dallas.	6
Модуль 4 **Цель:** знакомство с системой анализа рисков и проверки политики информационной безопасности предприятия	Система анализа рисков и проверки политики информационной безопасности предприятия.	6
Модуль 7 **Цель:** исследовать энергетическое скрытие речевой информации и скремблеры.	Энергетическое скрытие речевой информации. Скремблеры.	7

5.4. Практические работы

Таблица 4. Практические работы и их трудоемкость

Модули. Цели ПЗ	**Примерная тематика занятий и форма их проведений**	**Трудоемкость в часах**
Модуль 2 **Цель:** изучение стандартов информационной безопасности и критерии оценки безопасности систем и сетей передачи информации.	Стандарты информационной безопасности и критерии оценки безопасности систем и сетей передачи информации	7
Модуль 3 **Цель:** разработать архитектуру модели безопасности информационных систем и сетей.	Разработка архитектуры модели безопасности информационных систем и сетей	8

Модуль 4 **Цель:** разработать практические рекомендации по обеспечению безопасности информационных систем.	Разработка практических рекомендаций по обеспечению безопасности информационных систем	10
Модуль 5 **Цель:** изучение законодательства в области информационной безопасности.	Законодательство в области информационной безопасности	9
Модуль 7 **Цель:** изучение понятия и особенностей утечки информации. Исследование структуры, классификация и основные характеристики технических каналов утечки информации.	Понятие и особенности утечки информации. Структура, классификация и основные характеристики технических каналов утечки информации. Простые и составные технические каналы утечки информации. Характеристика и возможности оптических, акустических, радиоэлектронных и материально-вещественных каналов утечки информации	4

6. Самостоятельная работа обучающихся и текущий контроль их успеваемости

6.1. Цели самостоятельной работы

Формирование способностей к самостоятельному познанию и обучению, поиску литературы, обобщению, оформлению и представлению полученных результатов, их критическому анализу, поиску новых и неординарных решений, аргументированному отстаиванию своих предложений, умений подготовки выступлений и ведения дискуссий.

6.2. Организация и содержание самостоятельной работы

Самостоятельная работа заключается в изучении отдельных тем курса по заданию преподавателя по рекомендуемой им учебной литературе, в подготовке к лабораторным и практических работам, к текущему контролю успеваемости и подготовке к экзамену.

В рамках дисциплины выполняется 3 лабораторных работы и 5 практических, которые защищаются посредством тестирования или устным опросом (по желанию обучающегося). Максимальная оценка за каждую выполненную лабораторную работу – 5 баллов, минимальная – 3 балла.

Выполнение всех лабораторных работ обязательно. В случае невыполнения лабораторной работы по уважительной причине студент имеет право выполнить письменный реферат, по согласованной с преподавателем теме по модулю, по которому пропущена лабораторная работа.

Таблица 5. Темы рефератов.

№ п/п	Модули	Возможная тематика самостоятельной реферативной работы
1.	**Модуль 1**	Виды защищаемой информации.
		Роль информационной безопасности в обеспечении национальной безопасности государства.
2.	**Модуль 2**	Анализ угроз информационной безопасности.
		Защита от угрозы целостности на уровне содержания информации.
3.	**Модуль3**	Построение систем защиты от угрозы нарушения конфиденциальности информации.
		Цифровая подпись.
4.	**Модуль4**	Модель Харрисона-Руззо-Ульмана (HRU).
		Эквивалентные подходы к определению безопасности модели Белла-Лападулы.
5.	**Модуль5**	Классы защищенности АС.
		Стандарт оценки безопасности компьютерных систем TCSEC («Оранжевая книга»).
6.	**Модуль6**	Исследование корректности реализации и методы верификации АС.
		Центры компьютерной безопасности.
7.	**Модуль7**	Понятие и особенности утечки информации.
		Простые и составные технические каналы утечки информации.

7. Учебно-методическое и информационное обеспечение дисциплины

7.1. Основная литература по дисциплине

Радиоэлектронная защита объектов и информации : учебное пособие / В. В. Смирнов, Л. Б. Кочин, С. А. Певишев, А. С. Стукалова. — Санкт-Петербург : БГТУ "Военмех" им. Д.Ф. Устинова, 2020. — 38 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/172236 (дата обращения: 26.04.2023). — Режим доступа: для авториз. пользователей. - (ID=155301-0)

7.2. Дополнительная литература по дисциплине

1. Голиков, А. М. Защита информации от утечки по техническим каналам : учебное пособие / А. М. Голиков. — Москва : ТУСУР, 2015. — 256 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/110328 (дата обращения: 26.04.2023). — Режим доступа: для авториз. пользователей.- (ID=155302-0)
2. Голиков, А.М. Модуляция, кодирование и моделирование в телекоммуникационных системах. Теория и практика : учебное пособие / А.М. Голиков. - 3-е изд. ; стер. - Санкт-Петербург [и др.] : Лань, 2022. - ЭБС Лань. - Текст : электронный. - Режим доступа: по подписке. - Дата обращения: 07.07.2022. - ISBN 978-5-8114-9233-6. - URL: https://e.lanbook.com/book/189336 . - (ID=136012-0)
3. Горев, А. И. Обработка и защита информации в компьютерных системах : учебно-практическое пособие / А. И. Горев, А. А. Симаков. — Омск : Омская академия МВД России, 2016. — 88 с. — ISBN 978-5-88651-642-5. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/72856.html (дата обращения: 26.04.2023). — Режим доступа: для авторизир. пользователей - (ID=155303-0)

4. Ксендзов, А. В. Защищенные системы передачи информации : учебное пособие / А. В. Ксендзов. — Рязань : РГРТУ, 2021 — Часть 1 — 2021. — 96 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/310535 (дата обращения: 26.04.2023). — Режим доступа: для авториз. пользователей. - (ID=155304-0)
5. Прохорова, О.В. Информационная безопасность и защита информации : учебник для вузов / О.В. Прохорова. - 3-е изд. - Санкт-Петербург [и др.] : Лань, 2021. - ЭБС Лань. - Текст : электронный. - Режим доступа: по подписке. - Дата обращения: 07.07.2022. - ISBN 978-5-8114-7970-2. - URL: https://e.lanbook.com/book/169817 . - (ID=145977-0)
6. Зенков, А.В. Информационная безопасность и защита информации : учебное пособие для вузов / А.В. Зенков. - Москва : Юрайт, 2022. - (Высшее образование). - Образовательная платформа Юрайт. - Текст : электронный. - Режим доступа: по подписке. - Дата обращения: 07.07.2022. - ISBN 978-5-534-14590-8. - URL: https://urait.ru/bcode/497002 . - (ID=140920-0)
7. Пушкарев, В.В. Защита информационных процессов в компьютерных системах : учебное пособие / В.В. Пушкарев, В.П. Пушкарев; Томский государственный университет систем управления и радиоэлектроники. - Москва : Томский государственный университет систем управления и радиоэлектроники, 2012. - ЭБС Лань. - Текст : электронный. - Режим доступа: по подписке. - Дата обращения: 07.07.2022. - URL: https://e.lanbook.com/book/4925 . - (ID=145966-0)
8. Каширская, Е.Н. Защита информации в информационно-управляющих системах : учебное пособие / Е.Н. Каширская, М.А. Макаров; МИРЭА - Российский технологический университет. - Москва : МИРЭА - Российский технологический университет, 2020. - ЭБС Лань. - Текст : электронный. - Режим доступа: по подписке. - Дата обращения: 07.07.2022. - URL: https://e.lanbook.com/book/167621 . - (ID=145978-0)

7.3. Методические материалы

1. Учебно-методический комплекс дисциплины части, формируемой участниками образовательных отношений Блока 1 "Дисциплины (модули)" "Защита информации в радиотехнических системах". Направление подготовки специалистов - 11.05.01 Радиоэлектронные системы. Направленность (профиль) – Радиолокационные системы и комплексы : ФГОС 3++ / Каф. Радиотехнические и информационные системы ; сост. В.К. Кемайкин. - Тверь, 2022. - (УМК). - Текст : электронный. - URL: https://elib.tstu.tver.ru/MegaPro/GetDoc/Megapro/155299 . - (ID=155299-0)
2. Конспект лекций по дисциплине "Защита информации в информационных системах" направления подготовки 09.04.02 Информационные системы и технологии. Профиль: Радиотехнические системы и комплексы : в составе учебно-методического комплекса / Каф. Информационные системы ; разраб. В.В. Алексеев. - Тверь : ТвГТУ, 2017. - (УМК-Л). - Сервер. - Текст : электронный. - (ID=129676-0)

7.4. Программное обеспечение по дисциплине

Операционная система Microsoft Windows: лицензии № ICM-176609 и № ICM-176613 (Azure Dev Tools for Teaching).

Microsoft Office 2007 Russian Academic: OPEN No Level: лицензия № 41902814.

7.5. Специализированные базы данных, справочные системы, электронно-библиотечные системы, профессиональные порталы в Интернет

ЭБС и лицензионные ресурсы ТвГТУ размещены:

1. Ресурсы:https://lib.tstu.tver.ru/header/obr-res
2. ЭКТвГТУ:https://elib.tstu.tver.ru/MegaPro/Web
3. ЭБС "Лань":https://e.lanbook.com/
4. ЭБС "Университетская библиотека онлайн":https://www.biblioclub.ru/
5. ЭБС «IPRBooks»:https://www.iprbookshop.ru/
6. Электронная образовательная платформа "Юрайт" (ЭБС «Юрайт»):https://urait.ru/
7. Научная электронная библиотека eLIBRARY:https://elibrary.ru/
8. Информационная система "ТЕХНОРМАТИВ". Конфигурация "МАКСИМУМ" : сетевая версия (годовое обновление): [нормативно-технические, нормативно-правовые и руководящие документы (ГОСТы, РД, СНиПы и др.]. Диск 1,2,3,4. - М. :Технорматив, 2014. - (Документация для профессионалов). - CD. - Текст : электронный. - 119600 р. – (105501-1)
9. База данных учебно-методических комплексов:https://lib.tstu.tver.ru/header/umk.html

УМК размещен: https://elib.tstu.tver.ru/MegaPro/GetDoc/Megapro/155299

8. Материально-техническое обеспечение дисциплины

При изучении дисциплины «Защита информации в радиотехнических системах» используются современные средства обучения: наглядные пособия, диаграммы, схемы.

Возможна демонстрация лекционного материала с помощью оверхед-проектора (кодоскопа) и мультипроектора.

9. Оценочные средства для проведения промежуточной аттестации

9.1. Оценочные средства для проведения промежуточной аттестации в форме экзамена

1. Шкала оценивания промежуточной аттестации в форме экзамена – «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

2. Критерии оценки за экзамен:

для категории «знать»:

выше базового – 2;

базовый – 1;

ниже базового – 0.

Критерии оценки и ее значение для категории «уметь» (бинарный критерий):

отсутствие умения – 0 балл;

наличие умения – 2 балла.

«отлично» - при сумме баллов 5 или 6;
«хорошо» - при сумме баллов 4;
«удовлетворительно» - при сумме баллов 3;
«неудовлетворительно» - при сумме баллов 0, 1 или 2.

3. Вид экзамена – письменный экзамен.

4. Экзаменационный билет соответствует форме, утвержденной Положением о рабочих программах дисциплин, соответствующих федеральным государственным образовательным стандартам высшего образования с учетом профессиональных стандартов. Типовой образец экзаменационного билета приведен в Приложении. Обучающемуся даётся право выбора заданий из числа, содержащихся в билете, принимая во внимание оценку, на которую он претендует.

Число экзаменационных билетов – 21. Число вопросов (заданий) в экзаменационном билете – 3.

Продолжительность экзамена – 60 минут.

5. База заданий, предъявляемая обучающимся на экзамене.

1. Выделите два основных типа межсетевых экранов. Какие действия по умолчанию осуществляются межсетевым экраном в отношении трафика? Является ли один из типов межсетевых экранов более безопасным, нежели другой? Что межсетевой экран прикладного уровня по умолчанию делает с внутренними адресами?
2. В чем сходство межсетевого экрана с фильтрацией пакетов и маршрутизатора? Когда рекомендуется выбирать межсетевой экран с пакетной фильтрацией? Что должен обеспечивать межсетевой экран для проверки состояния? При каком условии межсетевой экран прикладного уровня может называться гибридным?
3. Угрозы информации. Виды угроз. Основные нарушения. Характер происхождения угроз. Источники угроз. Предпосылки появления угроз.
4. Что такое информационная безопасность? Какие компоненты входят в информационную безопасность?
5. Назовите два типа биометрических систем. Назовите основные категории атак.
6. Система защиты информации. Классы каналов несанкционированного получения информации. Причины нарушения целостности информации.
7. Методы и модели оценки уязвимости информации. Общая модель воздействия на информацию. Общая модель процесса нарушения физической целостности информации.
8. Структурированная схема потенциально возможных злоумышленных действий в автоматизированных системах обработки данных.
9. Для предотвращения перехвата должно использоваться шифрование - вместе с какой службой безопасности? Может ли служба обеспечения доступности предотвратить атаки на отказ в обслуживании?
10. Назовите три типа аутентификационных факторов. Почему двухфакторная аутентификация.
11. Методологические подходы к оценке уязвимости информации. Модель защиты системы. с полным перекрытием. Рекомендации по использованию моделей оценки уязвимости информации. Допущения в моделях оценки уязвимости информации.

12. Методы определения требований к защите информации. Факторы, обусловливающие конкретные требования к защите, обусловленные спецификой автоматизированной обработки информации. Классификация требований к средствам защиты информации.
13. Требования к защите, определяемые структурой автоматизированной системы обработки данных. Требования к защите, обусловливаемые видом защищаемой информации. Требования, обусловливаемые взаимодействием пользователя с комплексом средств автоматизации.
14. Должна ли политика безопасности определять конкретные требования реализации для каждого типа систем внутри самой политики? Почему в политику безопасности включают отказы от защиты?
15. Назовите две составляющих риска. Каков уровень риска при отсутствии угроз?
16. Назовите две составляющих риска. Каков уровень риска при отсутствии угроз? Что такое уязвимость? Назовите четыре цели для угроз. Может ли угроза иметь более одной цели?
17. Где расположены доступные из интернета системы в архитектуре с одним межсетевым экраном? Почему порядок правил в наборе правил межсетевого экрана играет важную роль?
18. Можно ли рассматривать использование SSH как реализацию VPN? Почему пользовательские VPN требуют строгой аутентификации?
19. Может ли шифрование полностью защитить данные, передаваемые через VPN. С чем необходимо комбинировать политику, чтобы обеспечить безопасность VPN?
20. Пригодны ли межузловые VPN для использования между организациями? Почему адресация является потенциальной проблемой, связанной с межузловыми VPN?
21. Анализ существующих методик определения требований к защите информации.
22. Факторы, влияющие на требуемый уровень защиты информации. Функции и задачи защиты информации. Основные положения механизмов непосредственной защиты и механизмы управления механизмами непосредственной защиты. Методы формирования функций защиты. События, возникающие при формировании функций защиты.
23. Если информация очень секретна, какой метод аутентификации следует использовать? Где должны храниться записи аудита в идеальном случае?
24. В чем сходство межсетевого экрана с фильтрацией пакетов и маршрутизатора? Когда рекомендуется выбирать межсетевой экран с пакетной фильтрацией
25. Какое скремблирование реализует данный скремблер? (аналоговое или цифровое). Какой вид частотного преобразования осуществляет данный скремблер?
26. Каковы преимущества и недостатки данного вида скремблирования? Какова разборчивость выходного сигнала? Какую полосу частот занимает выходной сигнал?

27. Способы и средства защиты информации. Способы «абсолютной системы защиты». Архитектура систем защиты информации. Требования. Общеметодологических принципов архитектуры системы защиты информации.
28. На каких системах должны устанавливаться антивирусные программы? Какой длины должны быть пароли?
29. Что должен обеспечивать межсетевой экран для проверки состояния? При каком условии межсетевой экран прикладного уровня может называться гибридным?
30. Согласно ГОСТ Р ИСО/МЭК 1 - какие три группы факторов необходимо учитывать при формировании требований в области информационной безопасности?
31. Какие основные информационные активы должны быть учтены и закреплены за ответственными владельцами для обеспечения информационной безопасности организации?
32. Ключевые моменты этапа анализа рисков: (перечислите)
33. Пригодны ли межузловые VPN для использования между организациями? Почему адресация является потенциальной проблемой, связанной с межузловыми VPN?
34. Какие два критерия должны использоваться для определения того, какое устройство следует использовать - межсетевой экран или VPN-сервер на отдельной системе? Если используется отдельный VPN-сервер, должен ли он размещаться в демилитаризованной зоне интернета?
35. Каким набором параметров может быть идентифицирован риск. По какой формуле может быть вычислена стоимость риска?
36. Перечислите стандарте ОК 11 классов функциональных требований.
37. Как производится вычисление потенциала нападения?
38. Можно ли рассматривать использование SSH как реализацию VPN? Почему пользовательские VPN требуют строгой аутентификации?
39. Стандарты информационной безопасности и критерии оценки безопасности систем и сетей передачи информации
40. Разработка архитектуры модели безопасности информационных систем и сетей
41. Разработка практических рекомендаций по обеспечению безопасности информационных систем
42. Законодательство в области информационной безопасности
43. Понятие и особенности утечки информации. Структура, классификация и основные характеристики технических каналов утечки информации.
44. Простые и составные технические каналы утечки информации.
45. Характеристика и возможности оптических, акустических, радиоэлектронных и материально-вещественных каналов утечки информации.

При ответе на вопросы экзамена допускается использование справочными данными, ГОСТами, методическими указаниями по выполнению лабораторных работ в рамках данной дисциплины.

Пользование различными техническими устройствами не допускается. При желании студента покинуть пределы аудитории во время экзамена экзаменационный билет после его возвращения заменяется.

Преподаватель имеет право после проверки письменных ответов на экзаменационные вопросы задавать студенту в устной форме уточняющие вопросы в рамках содержания экзаменационного билета, выданного студенту.

Иные нормы, регламентирующие процедуру проведения экзамена, представлены в Положении о текущем контроле успеваемости и промежуточной аттестации студентов.

9.2. Оценочные средства для проведения промежуточной аттестации в форме зачета

Учебным планом зачет по дисциплине не предусмотрен.

9.3. Оценочные средства для проведения промежуточной аттестации в форме курсового проекта или курсовой работы

Учебным планом курсовой проект или курсовая работа по дисциплине не предусмотрены.

10. Методические рекомендации по организации изучения дисциплины.

Студенты очной формы обучения перед началом изучения дисциплины должны быть ознакомлены с возможностью получения экзаменационной оценки по результатам текущей успеваемости, с формами защиты выполненных лабораторных и практических работ.

В учебном процесс рекомендуется внедрение субъект-субъектной педагогической технологии, при которой в расписании каждого преподавателя определяется время консультаций студентов по закрепленному за ним модулю дисциплины.

Рекомендуется обеспечить студентов, изучающих дисциплину, электронными учебниками, учебно-методическим комплексом по дисциплине, включая методические указания к выполнению всех видов самостоятельной работы.

11. Внесение изменений и дополнений в рабочую программу дисциплины

Кафедра ежегодно обновляет содержание рабочих программ дисциплин, которые оформляются протоколами заседаний дисциплин, форма которых утверждена Положением о рабочих программ дисциплин, соответствующих ФГОС ВО.

Приложение

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тверской государственный технический университет»

Направление подготовки специалистов – 11.05.01 Радиоэлектронные системы и комплексы

Направленность (профиль) – Радиолокационные системы и комплексы

Кафедра «Радиотехнические информационные системы»

Дисциплина «Защита информации в радиотехнических системах»

Семестр 10

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №_1__

1. Вопрос для проверки уровня «ЗНАТЬ» – 0 или 1 или 2 балла:

Что такое информационная безопасность? Какие компоненты входят в информационную безопасность?

2. Задание для проверки уровня «УМЕТЬ» по разделу «Методы защиты информации» - 0 или 2 балла:

Какие методы защиты информации используются в стандарте IEEE802.11 (WiFi):

1) PAW, EWR;
2) WER, WAP;
3) PEW, APW;
4) WEP, WPA.

3. Задание для проверки уровня «УМЕТЬ» по разделу «Модель управления доступом» - 0 или 2 балла:

Какая модель является моделью мандатного управлению доступом:

1) Модель Белла – ЛаПадула;
2) Модель Биба;
3) Хиррисона–Руззо-Ульмана;
4) Модель Кларка – Вилсона.

Критерии итоговой оценки за экзамен:

«отлично» - при сумме баллов 5 или 6;
«хорошо» - при сумме баллов 4;
«удовлетворительно» - при сумме баллов 3;
«неудовлетворительно» - при сумме баллов 0, 1 или 2.

Составитель: проф. кафедры РИС _____ В.К. Кемайкин

Заведующий кафедрой РИС _____ С.Ф. Боев