МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Самарский государственный технический университет»
(ФГБОУ ВО «СамГТУ»)

УТВЕРЖДАЮ:
Проректор по учебной работе
_____О.В. Юсупова
(подпись, ФИО)
«28» 10 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
ФТД.01 «Теория информационной безопасности и методология защиты информации»

(указывается шифр и наименование дисциплины по учебному плану)

Направление подготовки (специальность)	**11.04.01 «Радиотехника»** (код и наименование направления подготовки (специальности)
Направленность (профиль)	**Радиоэлектронные средства в системах безопасности** (наименование)
Квалификация	**Магистр**
Форма обучения	**очная** (очная, очно-заочная, заочная)
Год начала подготовки	**2023**
Институт / факультет	**Автоматики и Информационных Технологий**
Кафедра-разработчик	**Электронные системы и информационная безопасность** (наименование)
Объем дисциплины, ч. / з.е.	**72/2**
Форма контроля (промежуточная аттестация)	**Зачет с оценкой**

Самара
2022 г.

ФТД.01 «Теория информационной безопасности и методология защиты информации»

Рабочая программа дисциплины (далее – РПД) разработана в соответствии с требованиями ФГОС ВО по направлению подготовки (специальности) 11.04.01 «Радиотехника», утвержденного приказом Министерства образования и науки РФ от 19.09.2017 № 925-ФЗ, и соответствующего учебного плана.

Разработчик РПД:

доцент, к.т.н (должность, степень, ученое звание)	(подпись)	Мачихин В.А. (ФИО)
Заведующий кафедрой	к.т.н, доцент (степень, ученое звание, подпись)	Карпова Н.Е (ФИО)

СОГЛАСОВАНО:

Председатель методического совета *факультета / института (или учебно-методической комиссии)*	к.п.н (степень, ученое звание, подпись)	Стельмах Я.Г (ФИО)
Руководитель образовательной программы	д.т.н, ст.н.сотр (степень, ученое звание, подпись)	Скобелев П. О (ФИО)
Заведующий выпускающей кафедрой	к.т.н, доцент (степень, ученое звание, подпись)	Карпова Н.Е (ФИО)

СОДЕРЖАНИЕ

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Профессиональные компетенции

Таблица 1

Код и наименование компетенции	**Код и наименование индикатора достижения компетенции**	**Результаты обучения** (знать, уметь, владеть), **соотнесенные с индикаторами достижения компетенций**
ПК-1 Способен к проведению научно-исследовательских работ в области радиоэлектронных средств в системах информационной безопасности	ПК-1.1. Проводит поиск, изучение, обобщение и систематизацию информации, направленной на разработку и модернизацию радиоэлектронных средств и систем в области информационной безопасности	Знает: значение информационной безопасности и её место в системе национальной безопасности.
		Умеет: осуществлять правовое, организационное и инженерно-техническое обеспечение безопасности.
		Владеет: способностью к анализу направления обеспечения безопасности информационных систем
	ПК-1.2. Определяет основные этапы проведения научно исследовательских работ в области радиоэлектронных средств в системах информационной безопасности	Знает: теоретические и концептуальные основы защиты информации
		Умеет: осуществлять сбор и анализ информации в политической, военной, экономической областях деятельности
		Владеет: способность к нейтрализации угроз безопасности защищаемой информации.
	ПК-1.3. Проводит моделирование разрабатываемых радиоэлектронных систем	Знает: обобщенную модель информационного противоборства системы информационного нападения и системы защиты информации
		Умеет: находить и анализировать каналы несанкционированного получения информации.
		Владеет: навыками анализа зон злоумышленных действий в современных автоматизированных системах обработки данных
ПК-2 Способен разрабатывать и проектировать радиоэлектронные системы и узлы в системах информационной безопасности	ПК-2.1. Осуществляет анализ современной элементной базы, методов и принципов функционирования радиоэлектронных средств	Знает: направления, виды и особенности деятельности разведывательных служб по несанкционированному доступу к конфиденциальной информации
		Умеет: использовать методы теории нечетких множеств при моделировании систем защиты информации.
		Владеет: навыками анализа графов, матричных и множественных представлений межавтоматных связей в системе
	ПК-2.2. Разрабатывает технические решения для радиоэлектронных средств в системах безопасности	Знает: неформальные методы оценивания параметров моделируемых систем защиты информации
		Умеет: использовать неформальные методы поиска оптимальных решений
		Владеет: методологией определения требований к защите информации.
	ПК-2.3. Выполняет работы по подготовке технического задания для реализации радиоэлектронных систем и их узлов в системах информационной безопасности	Знает: модели прогнозирования значений показателей уязвимости
		Умеет: использовать общую модель исходов при осуществлении задач и функций обеспечения защиты информации.
		Владеет: способностью анализа обобщенных моделей системы защиты информации

2. Место дисциплины (модуля) в структуре образовательной программы

Дисциплина «Теория информационной безопасности и методология защиты информации» относится к факультативным дисциплинам учебного плана.

Таблица 2

Код компетенции	Предшествующие дисциплины	Параллельно осваиваемые дисциплины	Последующие дисциплины
ПК-1 Способен к проведению научно-исследовательских работ в области радиоэлектронных средств в системах информационной безопасности	Основы научно-исследовательской деятельности Теория систем и системный анализ Информационные технологии в радиоэлектронных системах	Мастерская инноваций (проектная мастерская)	Инженерное предпринимательство Методы и алгоритмы обработки изображений в системах безопасности Производственная практика: преддипломная практика Подготовка к процедуре защиты и защита выпускной квалификационной работы
ПК-2 Способен разрабатывать и проектировать радиоэлектронные системы и узлы в системах информационной безопасности		Основы проектирования систем безопасности на программируемых логических интегральных схемах Конструирование и технологии устройств сверхвысокой частоты Защищенные интерфейсы Интерфейсы радиоэлектронных устройств Системы радиолокации и радионавигации Средства радиоэлектронной борьбы в радиолокации и радионавигации	Антенно-фидерные устройства Производственная практика: преддипломная практика Подготовка к процедуре защиты и защита выпускной квалификационной работы

3. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Таблица 3

Вид учебной работы	Всего часов	Семестр 2 часов
Аудиторная контактная работа (всего), в том числе:	32	32
лекционные занятия (ЛЗ)	16	16
практические занятия (ПЗ)	16	16
Внеаудиторная контактная работа, КСР	3	3
Самостоятельная работа (всего), в том числе:	37	37
подготовка к практическим занятиям	37	37
ИТОГО: час.	**72**	**72**
ИТОГО: з.е.	**2**	**2**

4. Содержание дисциплины (модуля), структурированное по темам (разделам), с указанием отведенного на них количества академических часов и видов учебных занятий

Таблица 4

№ раздела	Наименование раздела дисциплины	Виды учебной нагрузки и их трудоемкость, часы				
		ЛЗ	ЛР	ПЗ	СРС	Всего часов
1	Сущность и понятие информационной безопасности	2		2	8	12

№ раздела	Наименование раздела дисциплины	Виды учебной нагрузки и их трудоемкость, часы				
		ЛЗ	ЛР	ПЗ	СРС	Всего часов
2	Основные положения и проблемы защиты информации	2		4	5	11
3	Каналы и методы несанкционированного доступа к информации	2		2	8	12
4	Методологический базис теории защиты информации	4		4	8	16
5	Модели систем и процессов защиты информации.	4		4	8	16
6	Кадровое и ресурсное обеспечение защиты информации	2		0	0	2
	КСР					3
	Итого:	**16**		**16**	**37**	**72**

4.1. Содержание лекционных занятий

Таблица 5

№ ЛЗ	Наименование раздела	Тема лекции	Содержание лекции (перечень дидактических единиц: рассматриваемых подтем, вопросов)	Количество часов
Семестр _2_				
1	Сущность и понятие информационной безопасности	Тема 1.1. Сущность информационной безопасности. Тема 1.2. Значение информационной безопасности и её место в системе национальной безопасности. Тема 1.3. Современная доктрина информационной безопасности Российской Федерации. Тема 1.4. Направления обеспечения безопасности информационных систем (ИС).	Определение понятия «информационная безопасность». Объекты информационной безопасности. Связь информационной безопасности с информатизацией общества. Структура информационной безопасности. Правовое, организационное и инженерно-техническое обеспечение безопасности.	2
2	Основные положения и проблемы защиты информации	Тема 2.1. Понятие и сущность защиты информации. Тема 2.2. Цели и значение защиты информации. Тема 2.3. Теоретические и концептуальные основы защиты информации. Тема 2.4. Критерии, условия и принципы отнесения информации к защищаемой. Тема 2.5. Угрозы безопасности защищаемой информации. Тема 2.6. Модели оценки потенциальных угроз.	Определение понятия «защита информации». Сущность защиты информации. Защита информации как составная часть информационной безопасности. Методологический подход к определению целей защиты информации. Место защиты информации в системе национальной безопасности. Значение защиты информации в политической, военной, экономической областях деятельности. Теория как основа концепции защиты информации. Становление и развитие государственной концепции защиты информации (для самостоятельного изучения). Понятие или свойство защищенности информации. Контур управления защитой информации. Обобщенная модель информационного противоборства системы информационного нападения и системы защиты информации.	2

№ ЛЗ	Наименование раздела	Тема лекции	Содержание лекции (перечень дидактических единиц: рассматриваемых подтем, вопросов)	Количество часов
			Условия, необходимые для отнесения информации к защищаемой (для самостоятельного изучения). Классификация угроз безопасности. Происхождения угроз. Взаимодействие параметров угроз информации. Причины нарушения целостности информации	
3	Каналы и методы несанкционированного доступа к информации	Тема 3.1. Каналы несанкционированного получения информации. Тема 3.2. Соотношения между каналами несанкционированного доступа к каналам утечки информации. Тема 3.3. Направления, виды и особенности деятельности разведывательных служб по несанкционированному доступу к конфиденциальной информации.	Классификации способов несанкционированного размножения информации. Зоны злоумышленных действий в современных автоматизированных системах обработки данных.	2
4	Методологический базис теории защиты информации	Тема 4.1. Теория нечетких множеств при моделировании систем защиты информации. Тема 4.2. Методология вероятностно-автоматного моделирования систем защиты.	Основные положения нестрогой математики при моделировании систем защиты информации. Графовое, матричное и множественное представление межавтоматных связей в системе.	2
5	Методологический базис теории защиты информации	Тема 4.3. Неформальные методы оценивания параметров моделируемых систем защиты информации. Тема 4.4. Неформальные методы поиска оптимальных решений. Тема 4.5. Методология определения требований к защите информации.	Неформальные методы оценивания параметров моделируемых систем защиты информации Неформальные методы поиска оптимальных решений Методология определения требований к защите информации.	2
6	Модели систем и процессов защиты информации.	Тема 5.1. Оценка уязвимости информации. Тема 5.2. Модели определения значений показателей уязвимости на технологических маршрутах автоматизированной обработки информации. Тема 5.3. Модели прогнозирования значений показателей уязвимости.	Оценка уязвимости информации Модели определения значений показателей уязвимости на технологических маршрутах автоматизированной обработки информации. Модели прогнозирования значений показателей уязвимости	2
7	Модели систем и процессов защиты информации.	Тема 5.4. Общая модель процесса защиты информации. Тема 5.5. Общая модель исходов при осуществлении задач и функций обеспечения защиты информации. Тема 5.6. Классификация методов и средств защиты	Обобщенная модель системы защиты информации. Общая модель исходов при осуществлении задач и функций обеспечения защиты информации. Классификация методов и средств защиты информации.	2

№ ЛЗ	Наименование раздела	Тема лекции	Содержание лекции (перечень дидактических единиц: рассматриваемых подтем, вопросов)	Количество часов
		информации.		
8	Кадровое и ресурсное обеспечение защиты информации	Тема 6. Полномочия по защите информации	Полномочия специальных комиссий по защите информации. Полномочия пользователей защищаемой информации. Значение ресурсного обеспечения для организации и эффективности защиты информации. Перспективы развития методов и средств компьютерной и комплексной защиты объектов информатизации. Проблемы в решении вопросов идеологии и технического обеспечения комплексной защиты объектов.	2
			Итого за семестр:	16
			Итого:	16

4.2. Содержание лабораторных занятий

Не предусмотрены учебным планом

4.3. Содержание практических занятий

Таблица 6

№ ПЗ	Наименование раздела	Тема практического занятия	Содержание практического занятия (перечень дидактических единиц: рассматриваемых подтем, вопросов)	Количество часов
Семестр 2				
1	Сущность и понятие информационной безопасности	**Практическое занятие № 1.** Современная доктрина информационной безопасности РФ.	Тема 1.3. Современная доктрина информационной безопасности Российской Федерации	2
2	Основные положения и проблемы защиты информации	**Практическое занятие № 2.** Понятие и сущность защиты информации	Тема 2.1. Понятие и сущность защиты информации. Определение понятия «защита информации». Сущность защиты информации. Защита информации как составная часть информационной безопасности.	2
3	Основные положения и проблемы защиты информации	**Практическое занятие № 3.** Угрозы безопасности защищаемой информации	Тема 2.5. Угрозы безопасности защищаемой информации. Классификация угроз безопасности. Происхождения угроз. Взаимодействие параметров угроз информации. Причины нарушения целостности информации	2
4	Каналы и методы несанкционированного доступа к информации	**Практическое занятие №4.** Каналы несанкционированного получения информации	Тема 3.1. Каналы несанкционированного получения информации. Классификации способов несанкционированного размножения информации. Зоны злоумышленных действий в современных автоматизированных системах обработки данных.	2
5	Методологический базис теории защиты информации	**Практическое занятие №5.** Методология вероятностно-автоматного моделирования систем защиты.	Тема 4.2. Методология вероятностно-автоматного моделирования систем защиты. Графовое, матричное и множественное представление межавтоматных связей в системе.	2
6	Методологический базис теории защи-	**Практическое занятие №6.** Методология определения требований к	Тема 4.5. Методология определения требований к защите информации.	2

№ ПЗ	Наименование раздела	Тема практического занятия	Содержание практического занятия (перечень дидактических единиц: рассматриваемых подтем, вопросов)	Количество часов
	ты информации	защите информации.		
7	Модели систем и процессов защиты информации.	**Практическое занятие №7.** Классификация методов защиты информации. защиты информации.	Тема 5.6. Общая модель исходов при осуществлении задач и функций обеспечения	2
8	Модели систем и процессов защиты информации.	**Практическое занятие №8.** Классификация средств защиты информации.	Тема 5.6. Общая модель исходов при осуществлении задач и функций обеспечения защиты информации.	2
			Итого за семестр:	16
			Итого:	16

4.4. Содержание самостоятельной работы

Таблица 7

Наименование раздела	Вид самостоятельной работы	Содержание самостоятельной работы (перечень дидактических единиц: рассматриваемых подтем, вопросов)	Количество часов
Семестр 2			
Сущность и понятие информационной безопасности	*Подготовка к практическому занятию*	*Подготовка к практическому занятию № 1. Современная доктрина информационной безопасности РФ.* Тема 1.3. Современная доктрина информационной безопасности Российской Федерации.	8
Основные положения и проблемы защиты информации	*Подготовка к практическому занятию*	*Подготовка к практическому занятию № 2. Понятие и сущность защиты информации* Тема 2.1. Понятие и сущность защиты информации. Определение понятия «защита информации». Сущность защиты информации. Защита информации как составная часть информационной безопасности.	2
Основные положения и проблемы защиты информации	*Подготовка к практическому занятию*	*Подготовка к практическому занятию № 3. Угрозы безопасности защищаемой информации* Тема 2.5. Угрозы безопасности защищаемой информации. Классификация угроз безопасности. Происхождения угроз. Взаимодействие параметров угроз информации. Причины нарушения целостности информации	3
Каналы и методы несанкционированного доступа к информации	*Подготовка к практическому занятию*	*Подготовка к практическому занятию №4. Каналы несанкционированного получения информации* Тема 3.1. Каналы несанкционированного получения информации. Классификации способов несанкционированного размножения информации. Зоны злоумышленных действий в современных автоматизированных системах обработки данных.	8
Методологический базис теории защиты информации	*Подготовка к практическому занятию*	*Подготовка к практическому занятию №5. Методология вероятностно-автоматного моделирования систем защиты.* Тема 4.2. Методология вероятностно-автоматного моделирования систем защиты. Графовое, матричное и множественное представление межавтоматных связей в системе.	4
Методологический базис теории защиты	*Подготовка к практическому занятию*	*Подготовка к практическому занятию №6. Методология определения требований к защите информации.* Тема 4.5. Методология определения требований к	4

Наименование раздела	Вид самостоятельной работы	Содержание самостоятельной работы (перечень дидактических единиц: рассматриваемых подтем, вопросов)	Количество часов
информации		защите информации.	
Модели систем и процессов защиты информации	*Подготовка к практическому занятию*	*Подготовка к практическому занятию №7.* Классификация методов защиты информации. Тема 5.6. Общая модель исходов при осуществлении задач и функций обеспечения защиты информации.	4
Модели систем и процессов защиты информации	*Подготовка к практическому занятию*	*Подготовка к практическому занятию №8.* Классификация средств защиты информации. Тема 5.6. Общая модель исходов при осуществлении задач и функций обеспечения защиты информации.	4
		Итого за семестр:	**37**
		Итого:	**37**

5. Перечень учебной литературы и учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

Таблица 8

№ п/п	Библиографическое описание	Ресурс НТБ СамГТУ (ЭБС СамГТУ, IPRbooks и т.д.)
Основная литература		
1	Фомин Д.В. Информационная безопасность; Вузовское образование, 2018.- Режим доступа: https://elib.samgtu.ru/getinfo?uid=els_samgtu||iprbooks||77320	ЭБС СамГТУ
2	Галатенко В.А. Основы информационной безопасности; Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020.- Режим доступа: https://elib.samgtu.ru/getinfo?uid=els_samgtu||iprbooks||97562	ЭБС СамГТУ
Дополнительная литература		
3	Рогозин В.Ю., Галушкин И.Б., Новиков В.К., Вепрев С.Б. Основы информационной безопасности; ЮНИТИ-ДАНА, 2017.- Режим доступа: https://elib.samgtu.ru/getinfo?uid=els_samgtu||iprbooks||72444	ЭБС СамГТУ
4	Башлы П.Н., Бабаш А.В., Баранова Е.К. Информационная безопасность и защита информации; Евразийский открытый институт, 2012.- Режим доступа: https://elib.samgtu.ru/getinfo?uid=els_samgtu||iprbooks||10677	ЭБС СамГТУ
Учебно-методическое обеспечение		
5	Учебно-методическое пособие по написанию курсовой работы по дисциплине Теория информационной безопасности и методология защиты инфокоммуникаций; Московский технический университет связи и информатики, 2016.- Режим доступа: https://elib.samgtu.ru/getinfo?uid=els_samgtu||iprbooks||61560	ЭБС СамГТУ
65	Методические указания по дисциплине Информационная безопасность; Московский технический университет связи и информатики, 2013.- Режим доступа: https://elib.samgtu.ru/getinfo?uid=els_samgtu||iprbooks||61736]	ЭБС СамГТУ

Доступ обучающихся к ЭР НТБ СамГТУ (elib.samgtu.ru) осуществляется посредством электронной информационной образовательной среды университета и сайта НТБ СамГТУ по логину и паролю.

6. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения

При проведении лекционных занятий используется мультимедийное оборудование..

Организовано взаимодействие обучающегося и преподавателя с использованием электронной информационной образовательной среды университета.

Таблица 9

№ п/п	Наименование	Производитель	Способ распространения
1	Операционная система Windows 10	Microsoft	лицензионное
2	Операционная система Astra Linux Special Edition	ГК Astra Linux (ООО «РусБИТех-Астра»)	лицензионное
3	Kaspersky Endpoint Security 11.6.0.394	Лаборатория Кас-	лицензионное

№ п/п	Наименование	Производитель	Способ распространения
		перского	
4	MaxPatrol Education	Positive Technologies	лицензионное
5	MaxPatrol SIEM Education	Positive Technologies	лицензионное
6	OpenOffice 3.2	Apache Software Foundation	свободно распространяемое
7	Средство просмотра PDF-файлов PDF24 10.0.10	Geek Software GmbH	свободно распространяемое
8	Средство просмотра DJVU-файлов WinDjView 2.1	Андрей и Леонид Жежерун	свободно распространяемое

7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», профессиональных баз данных, информационно-справочных систем

Таблица 10

№ п/п	Наименование	Краткое описание	Режим доступа
1	Электронная библиотека «Наука и техника»	http://n-t.ru/	Российские базы данных ограниченного доступа
2	Научно-электронная библиотека	http://elibrary.ru	Российские базы данных ограниченного доступа
3	Электронная библиотека изданий ФГБОУ ВО «СамГТУ»	http://lib.sumgtu.ru/	Российские базы данных ограниченного доступа
4	Электронно-библиотечная система "IPRbooks"	http://www.iprbookshop.ru/	Российские базы данных ограниченного доступа
5	Журнал Вестник СамГТУ. Серия «Технические науки».	http://vestnik-teh.samgtu.ru/	Ресурсы открытого доступа
6	Электронная библиотека Microsoft	http://msdn.microsoft.com/ru-ru/library	Ресурсы открытого доступа
7	Открытый университет	http://www.intuit.ru/	Ресурсы открытого доступа
8	РОСПАТЕНТ	http://www1.fips.ru	Ресурсы открытого доступа (открытые базы данных)
9	Консультант плюс	http://www.consultant.ru/	Ресурсы открытого доступа (открытые базы данных)
10	ГАРАНТ	http://www.garant.ru/	Ресурсы открытого доступа (открытые базы данных)

8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

Лекционные занятия

Аудитория для проведения лекционных занятий, оснащена мультимедийным оборудованием (ноутбук, колонки, настенный проекционный экран, проектор), с выходом в сеть Интернет и доступом в электронную информационно-образовательную среду СамГТУ. Аудитория оборудована специализированной мебелью: столы и стулья для обучающихся; стол и стул для преподавателя, доска.

Практические занятия

Аудитория для проведения практических занятий, оснащена мультимедийным оборудованием (ноутбук, колонки, настенный проекционный экран, проектор), с выходом в сеть Интернет и доступом в электронную информационно-образовательную среду СамГТУ. Аудитория оборудована специализированной мебелью: столы и стулья для обучающихся; стол и стул для преподавателя, доска.

Самостоятельная работа

Аудитория для самостоятельной работы, оснащена компьютерной техникой с подключением к сети Интернет и доступом в электронную информационно-образовательную среду СамГТУ; учебной мебелью: столы, стулья для обучающихся, стол и стул для преподавателя; читальный зал НТБ СамГТУ (аудитория 125, корпус №1).

9. Методические материалы

В учебном процессе применяются следующие пассивные (лекции) и активные (практические занятия/подготовка к зачету) образовательные технологии.

Таблица 8

Вид учебных занятий	Организация деятельности студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии.
Практические занятия	Проработка рабочей программы, уделяя особое внимание целям и задачам структуре и содержанию дисциплины. Конспектирование источников. Работа с конспектом лекций, самостоятельное изучение теоретического материала, выступление с докладом по результатам подготовки к практическим занятиям с представлением иллюстрационного материала в виде презентации Microsoft PowerPoint.
Подготовка к зачету с оценкой	При подготовке к зачету с оценкой необходимо ориентироваться на конспекты лекций, рекомендуемую литературу, материалы практических занятий.

Лекция представляет собой систематическое устное изложение учебного материала. С учетом целей и места в учебном процессе различают лекции вводные, установочные, текущие, обзорные и заключительные. В зависимости от способа проведения выделяют лекции:

- *информационные;*
- *проблемные;*
- *визуальные;*
- *бинарные (лекция-диалог);*
- *лекции-провокации;*
- *лекции-конференции;*
- *лекции-консультации;*
- *лекции-беседы;*
- *лекция с эвристическими элементами;*
- *лекция с элементами обратной связи;*
- *лекция с решением производственных и конструктивных задач;*
- *лекция с элементами самостоятельной работы студентов;*
- *лекция с решением конкретных ситуаций;*
- *лекция с коллективным исследованием;*
- *лекции спецкурсов.*

Лекции по настоящей дисциплине проводятся в форме информационных, т.е. с использованием объяснительно иллюстративного метода изложения.

Перед началом лекции до обучающихся доводятся основные литературные источники, сообщается тема лекции и последовательность вопросов, подлежащих рассмотрению. При этом обращается внимание на логику построения вопросов, их формулировку и взаимосвязь.

По ходу лекции при возникновении проблемных вопросов (или ситуаций) процесс познания происходит через научный поиск, диалог, анализ, сравнение разных точек зрения.

При объяснении различных вопросов большое значение имеет иллюстрационный материал (формы документов, структур систем управления и проч.), поэтому в случае их сложного или долгого воспроизводства на лекции используется раздаточный материал.

Обращается внимание на вопросы, сведения из которых будут использоваться при проведении практических и лабораторных занятий и самостоятельной работе студентов. В Рабочей программе приводится содержание лекций и вопросы, выносимые на самостоятельное изучение с учётом дидактических единиц.

В некоторых случаях преподавателем может использоваться способ индивидуального общения, построенный на непосредственном контакте преподавателя и студента, который позволяет привлекать к двухстороннему обмену мнениями по наиболее важным вопросам темы занятия, менять темп изложения с учетом особенности аудитории.

В начале лекции и по ходу ее преподаватель задает слушателям вопросы не для контроля усвоения знаний, а для выяснения уровня осведомленности по рассматриваемой проблеме. Вопросы могут быть элементарными: для того, чтобы сосредоточить внимание, как на отдельных нюансах темы, так и на проблемах. Продумывая ответ, студенты получают возможность самостоятельно прийти к выводам и обобщениям, которые хочет сообщить преподаватель в качестве новых знаний. При этом необходимо следить, чтобы вопросы не оставались без ответа, иначе лекция будет носить риторический характер.

Обратная связь устанавливается посредством ответов студентов на вопросы преподавателя по ходу лекции. Чтобы определить осведомленность студентов по излагаемой проблеме, в начале какого-либо раздела лекции задаются необходимые вопросы.

Если студенты правильно отвечают на вводный вопрос, преподаватель может ограничиться кратким тезисом или выводом и перейти к следующему вопросу. Если же ответы не удовлетворяют уровню желаемых знаний, преподаватель сам излагает подробный ответ, и в конце объяснения снова задает вопрос,

определяя степень усвоения учебного материала.

Рекомендации обучающимся при работе с лекционным материалом:

1. Материал каждой законспектированной лекции должен прочитываться и прорабатываться с выявлением затрудненных в понимании вопросов и неясностей.
2. Необходимо попытаться добиться ясности понимания с использованием проработки рекомендованных литературных источников.
3. Если и в этом случае не удаётся добиться результата, то следует получить консультацию преподавателя по этому вопросу.
4. Следует посмотреть, как этот вопрос формулируется в вопросах для подготовки к экзамену и быть готовым представить по нему информацию при проведении экзамена.

Практическое занятие — форма организации обучения, которая направлена на формирование практических умений и навыков и является связующим звеном между самостоятельным теоретическим освоением студентами учебной дисциплины и применением ее положений на практике.

Практические занятия по дисциплине проводятся в целях выработки практических умений и приобретения навыков в решении управленческих задач, выполнении заданий, разработке и оформлении документов, практического овладения компьютерными технологиями. Главным их содержанием является практическая работа каждого студента.

Подготовка студентов к практическому занятию – один из видов самостоятельной работы в рамках данной дисциплины. Подготовка производится по вопросам, разработанным для каждой темы практических занятий. Данная информация доводится до студентов заранее. По желанию обучающихся, они могут не только составить конспект по материалам подготовки к практическому занятию, но и подготовить доклад по соответствующей теме, которая формулируется самим обучающимся и согласуется с преподавателем. Доклад иллюстрируется с помощью презентации Microsoft PowerPoint. Рекомендации по выполнению самостоятельной работы представлены в соответствующих методических указаниях.

Работа студентов во время практического занятия осуществляется на основе заданий, которые выдаются обучающимся в начале занятия. Предварительно преподаватель проводит устный опрос по материалам подготовки к практическому занятию.

Практические занятия составляют значительную часть всего объема аудиторных занятий и имеют важнейшее значение для усвоения программного материала. Выполняемые задания могут быть:

1) иллюстрацией теоретического материала и носить воспроизводящий характер; они выявляют качество понимания студентами теории;

2) образцами задач и примеров, разобранных в аудитории; для самостоятельного выполнения требуется, чтобы студент овладел показанными методами решения;

3) видом заданий, содержащим элементы творчества; одни из них требуют от студента обобщений, для их выполнения необходимо привлекать ранее приобретенный опыт, устанавливать внутрипредметные и межпредметные связи; решение других требует дополнительных знаний, которые студент должен приобрести самостоятельно; третьи предполагают наличие у студента некоторых исследовательских умений;

4) может применяться выдача индивидуальных или опережающих заданий на различный срок, определяемый преподавателем, с последующим представлением их для проверки в указанный срок.

По данной дисциплине предусмотрено проведение 18 практических занятий длительностью 2 академических часа каждое. Темы практических занятий приведены в Разделе 3.2 Рабочей программы.

В начале занятия рассматриваются основные теоретические положения, положенные в основу занятия. Обращается внимание на основные понятия, расчетные формулы, алгоритмы, практическую значимость рассматриваемых вопросов. Далее студентам предлагаются определенные условия (задачи), для которых требуется выполнить расчет определенных параметров или выработать определенные технологические решения. Задания могут быть групповые и индивидуальные. В зависимости от сложности предлагаемых заданий, целей занятия, общей подготовки обучающихся преподаватель может подсказать обучающимся алгоритм решения, или первое действие, или указать общее направление рассуждений. Полученные результаты обсуждаются с позиций их адекватности или эффективности в рассмотренной ситуации.

10. Фонд оценочных средств по дисциплине (модулю)

по дисциплине

ФТД.01 «Теория информационной безопасности и методология защиты информации»

Код и направление подготовки (специальность)	**11.04.01 Радиотехника**
Направленность (профиль)	**Радиоэлектронные средства в системах безопасности**
Квалификация	**магистр**
Форма обучения	**очная**
Год начала подготовки	**2023**
Институт / факультет	**Автоматики и Информационных Технологий**
Выпускающая кафедра	**Электронные системы и информационная безопасность**
Кафедра-разработчик	**Электронные системы и информационная безопасность**
Объем дисциплины, ч. / з.е.	**72/2**
Форма контроля (промежуточная аттестация)	**Зачет с оценкой**

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Профессиональные компетенции

Таблица 1

Код и наименование компетенции	**Код и наименование индикатора достижения компетенции**	**Результаты обучения** (знать, уметь, владеть), **соотнесенные с индикаторами достижения компетенций**
ПК-1 Способен к проведению научно-исследовательских работ в области радиоэлектронных средств в системах информационной безопасности	ПК-1.1. Проводит поиск, изучение, обобщение и систематизацию информации, направленной на разработку и модернизацию радиоэлектронных средств и систем в области информационной безопасности	Знает: значение информационной безопасности и её место в системе национальной безопасности.
		Умеет: осуществлять правовое, организационное и инженерно-техническое обеспечение безопасности.
		Владеет: способностью к анализу направления обеспечения безопасности информационных систем
	ПК-1.2. Определяет основные этапы проведения научно исследовательских работ в области радиоэлектронных средств в системах информационной безопасности	Знает: теоретические и концептуальные основы защиты информации
		Умеет: осуществлять сбор и анализ информации в политической, военной, экономической областях деятельности
		Владеет: способность к нейтрализации угроз безопасности защищаемой информации.
	ПК-1.3. Проводит моделирование разрабатываемых радиоэлектронных систем	Знает: обобщенную модель информационного противоборства системы информационного нападения и системы защиты информации
		Умеет: находить и анализировать каналы несанкционированного получения информации.
		Владеет: навыками анализа зон злоумышленных действий в современных автоматизированных системах обработки данных
ПК-2 Способен разрабатывать и проектировать радиоэлектронные системы и узлы в системах информационной безопасности	ПК-2.1. Осуществляет анализ современной элементной базы, методов и принципов функционирования радиоэлектронных средств	Знает: направления, виды и особенности деятельности разведывательных служб по несанкционированному доступу к конфиденциальной информации
		Умеет: использовать методы теории нечетких множеств при моделировании систем защиты информации.
		Владеет: навыками анализа графов, матричных и множественных представлений межавтоматных связей в системе
	ПК-2.2. Разрабатывает технические решения для радиоэлектронных средств в системах безопасности	Знает: неформальные методы оценивания параметров моделируемых систем защиты информации
		Умеет: использовать неформальные методы поиска оптимальных решений
		Владеет: методологией определения требований к защите информации.
	ПК-2.3. Выполняет работы по подготовке технического задания для реализации радиоэлектронных систем и их узлов в системах информационной безопасности	Знает: модели прогнозирования значений показателей уязвимости
		Умеет: использовать общую модель исходов при осуществлении задач и функций обеспечения защиты информации.
		Владеет: способностью анализа обобщенных моделей системы защиты информации

Матрица соответствия оценочных средств запланированным результатам обучения

Таблица 2

Код и индикатор достижения компетенции	Оценочные средства						
	Раздел 1. Сущность и понятие информационной безопасности	**Раздел 2. Основные положения и проблемы защиты информации**	**Раздел 3. Каналы и методы несанкционированного доступа к информации**	**Раздел 4. Методологический базис теории защиты информации**	**Раздел 5. Модели систем и процессов защиты информации**	**Раздел 6. Кадровое и ресурсное обеспечение защиты информации**	**Зачет с оценкой**
	Собеседование на практических занятиях						Вопросы к зачету с оценкой
ПК-1.1	ПК-1.1. З1 ПК-1.1. У1 ПК-1.1. В1	ПК-1.1. З1 ПК-1.1. У1 ПК-1.1. В1	ПК-1.1. З1 ПК-1.1. У1 ПК-1.1. В1	ПК-1.1. З1 ПК-1.1. У1 ПК-1.1. В1	ПК-1.1. З1 ПК-1.1. У1 ПК-1.1. В1	ПК-1.1. З1 ПК-1.1. У1 ПК-1.1. В1	ПК-1.1. З1 ПК-1.1. У1 ПК-1.1. В1
ПК-1.2	ПК-1.2. З1 ПК-1.2. У1 ПК-1.2. В1	ПК-1.2. З1 ПК-1.2. У1 ПК-1.2. В1	ПК-1.2. З1 ПК-1.2. У1 ПК-1.2. В1	ПК-1.2. З1 ПК-1.2. У1 ПК-1.2. В1	ПК-1.2. З1 ПК-1.2. У1 ПК-1.2. В1	ПК-1.2. З1 ПК-1.2. У1 ПК-1.2. В1	ПК-1.2. З1 ПК-1.2. У1 ПК-1.2. В1
ПК-1.3	ПК-1.3. З1 ПК-1.3. У1 ПК-1.3. В1	ПК-1.3. З1 ПК-1.3. У1 ПК-1.3. В1	ПК-1.3. З1 ПК-1.3. У1 ПК-1.3. В1	ПК-1.3. З1 ПК-1.3. У1 ПК-1.3. В1	ПК-1.3. З1 ПК-1.3. У1 ПК-1.3. В1	ПК-1.3. З1 ПК-1.3. У1 ПК-1.3. В1	ПК-1.3. З1 ПК-1.3. У1 ПК-1.3. В1
ПК-2.1	ПК-2.1. З1 ПК-2.1. У1 ПК-2.1. В1	ПК-2.1. З1 ПК-2.1. У1 ПК-2.1. В1	ПК-2.1. З1 ПК-2.1. У1 ПК-2.1. В1	ПК-2.1. З1 ПК-2.1. У1 ПК-2.1. В1	ПК-2.1. З1 ПК-2.1. У1 ПК-2.1. В1	ПК-2.1. З1 ПК-2.1. У1 ПК-2.1. В1	ПК-2.1. З1 ПК-2.1. У1 ПК-2.1. В1
ПК-2.2	ПК-2.2. З1 ПК-2.2. У1 ПК-2.2. В1	ПК-2.2. З1 ПК-2.2. У1 ПК-2.2. В1	ПК-2.2. З1 ПК-2.2. У1 ПК-2.2. В1	ПК-2.2. З1 ПК-2.2. У1 ПК-2.2. В1	ПК-2.2. З1 ПК-2.2. У1 ПК-2.2. В1	ПК-2.2. З1 ПК-2.2. У1 ПК-2.2. В1	ПК-2.2. З1 ПК-2.2. У1 ПК-2.2. В1
ПК-2.3	ПК-2.3. З1 ПК-2.3. У1 ПК-2.3. В1	ПК-2.3. З1 ПК-2.3. У1 ПК-2.3. В1	ПК-2.3. З1 ПК-2.3. У1 ПК-2.3. В1	ПК-2.3. З1 ПК-2.3. У1 ПК-2.3. В1	ПК-2.3. З1 ПК-2.3. У1 ПК-2.3. В1	ПК-2.3. З1 ПК-2.3. У1 ПК-2.3. В1	ПК-2.3. З1 ПК-2.3. У1 ПК-2.3. В1

2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие процесс формирования компетенций в ходе освоения образовательной программы.

2.1. Формы текущего контроля успеваемости

Перечень практических занятий, по темам которых проводятся собеседования, представлен *в таблице 6* основной части рабочей программы дисциплины.

2.2. Формы промежуточной аттестации

Вопросы к зачету с оценкой

1. Проблемные вопросы в области информационной безопасности.
2. Основные направления обеспечения безопасности.
3. Понятие информатизации, её компоненты. Понятие информации, её свойства.
4. Три подхода к организации защиты информации.
5. Системный подход к организации защиты информации.
6. Иерархическая взаимосвязь основных свойств ИС АСУ.
7. Контур управления защитой информации.
8. Обобщенная модель информационного противоборства.
9. Классификация угроз безопасности.
10. Происхождения и содержания угроз информации.
11. Классификация и содержания угроз информации.
12. Каналы несанкционированного получения информации (КНПИ).
13. Классификация возможных способов несанкционированного размножения информации.
14. Модель процесса нарушения физической целостности информации. Зоны злоумышленных действий.
15. Определение уровня затрат и уровня защищенности информации (эмпирическая модель оценки фирмы IBM).
16. Динамическая модель оценки потенциальных угроз.
17. Модель системы защиты с полным перекрытием.

18. Оценка уязвимости информации (при территориально несанкционированном действии злоумышленника).
19. Модели определения показателей уязвимости для участков технологического процесса. (Линейный и Циклический участки).
20. Определение показателя уязвимости на ветвящемся участке технологического процесса.
21. Модели прогнозирования значений показателей уязвимости информации.
22. Рекомендации по использованию моделей прогнозирования.
23. Определения и основные понятия теории защиты информации, задачи ЗИ.
24. Методологические принципы защиты информации. (Основные принципы общетеоретического характера, теоретико-прикладные принципы).
25. Основные положения теории нечетких множеств.
26. Основные положения нестрогой математики.
27. Неформальные методы оценивания информации.
28. Методология вероятностно-автоматного моделирования. (Матричное представление и множественное представление).
29. Неформальные методы поиска оптимальных решений.
30. Эволюционное моделирование.
31. Общая модель процессов защиты информации.
32. Общая модель процессов защиты информации.
33. Унифицированная концепция защиты информации.

3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующие процесс формирования компетенций

Учебная дисциплина формирует компетенции в соответствии с табл. 2, процедура оценивания представлена в табл. 3 и реализуется поэтапно:

Характеристика процедур текущей и промежуточной аттестации по дисциплине

Таблица 3

№	Наименование оценочного средства*	Периодичность и способ проведения процедуры оценивания	Методы оценивания	Виды выставляемых оценок	Способ учета индивидуальных достижений обучающихся
1.	Собеседование на практических занятиях	Систематически на практических занятиях / устно	экспертный	По пятибалльной шкале	Рабочая книжка преподавателя
2.	Зачет с оценкой	По окончании изучения дисциплины; устно	экспертный	По пятибалльной шкале	Зачетная ведомость, зачетные книжки и учебные карточки, портфолио в АИС ВУЗа

Критерии и шкала оценивания результатов изучения дисциплины на промежуточной аттестации

Шкала оценивания:

«Отлично» – выставляется, если сформированность заявленных индикаторов компетенций 90% более (в соответствии с картами компетенций ОП): обучающийся показал прочные знания основных положений фактического материала, умение самостоятельно решать конкретные практические задачи повышенной сложности, свободно использовать справочную литературу, делать обоснованные выводы из результатов анализа конкретных ситуаций;

«Хорошо» – выставляется, если сформированность заявленных индикаторов компетенций на 80% и более (в соответствии с картами компетенций ОП): обучающийся показал прочные знания основных положений фактического материала, умение самостоятельно решать конкретные практические задачи, предусмотренные рабочей программой, ориентироваться в рекомендованной справочной литературе, умеет правильно оценить полученные результаты анализа конкретных ситуаций;

«Удовлетворительно» – выставляется, если сформированность заявленных индикаторов компетенций 60% и более (в соответствии с картами компетенций ОП): обучающийся показал знание основных положений фактического материала, умение получить с помощью преподавателя правильное решение конкретной практической задачи из числа предусмотренных рабочей программой, знакомство с рекомендованной справочной литературой;

«Неудовлетворительно» – выставляется, если сформированность заявленных индикаторов компетенций менее чем 59% (в соответствии с картами компетенций ОП): при ответе обучающегося выявились существенные пробелы в знаниях основных положений фактического материала, неумение с помощью

преподавателя получить правильное решение конкретной практической задачи из числа предусмотренных рабочей программой учебной дисциплины.

УТВЕРЖДАЮ
Проректор по учебной работе
_____ (Ф.И.О)
(подпись)
«____»_____ 20__ г.

Дополнения и изменения к рабочей программе дисциплины (модуля)

ФТД.01 «Теория информационной безопасности и методология защиты информации»

по направлению подготовки (специальности) *11.04.01 Радиотехника* по направленности (профилю) подготовки *Радиоэлектронные средства в системах безопасности*

на 20__/20__ уч.г.

В рабочую программу вносятся следующие изменения:

1) ……..;
2) ……..

Разработчик дополнений и изменений:

_____	_____	_____
(должность, степень, ученое звание)	(подпись)	(ФИО)

Дополнения и изменения рассмотрены и одобрены на заседании кафедры «____»_____ 20___ г., протокол № ____.

Заведующий кафедрой

_____	_____
(степень, звание, подпись)	(ФИО)