МИНОБРНАУКИ РОССИИ

федеральное государственное бюджетное образовательное учреждение
высшего образования
«ИРКУТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ФГБОУ ВО «ИГУ»
Кафедра радиофизики и радиоэлектроники

УТВЕРЖДАЮ:
Декан _____ Буднев Н.М.
«06» мая 2022 г.

Рабочая программа дисциплины

Наименование дисциплины **Б1.В.ДВ.01.01 Комплексное обеспечение информационной безопасности автоматизированных систем**

Направление подготовки **10.03.01 Информационная безопасность**

Направленность (профиль) подготовки **Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)**

Квалификация выпускника **бакалавр**

Форма обучения **очная**

Согласовано с УМК физического факультета

Протокол №32 от «23» марта 2022 г.

Председатель _____ Буднев Н.М.

Рекомендовано кафедрой радиофизики и радиоэлектроники:

Протокол № 6 от «01» марта 2022 г.

И.О. зав. кафедрой _____ Колесник С.Н.

Иркутск 2022 г

Содержание

стр.

I. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

Цели и задачи дисциплины «Комплексное обеспечение информационной безопасности автоматизированных систем»

Цели: Главной целью дисциплины является формирования у обучающихся универсальных, общепрофессиональных и профессиональных компетенций в соответствии с требованиями ФГОС ВО по направлению подготовки 10.03.01 **«Информационная безопасность»** направленность (профиль) «**Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)»,** а также изучение теоретических, методологических и практических проблем комплексного обеспечение информационной безопасности автоматизированных систем, формирования, функционирования и развития систем управления информационной безопасностью и комплексной защитой информации

Задачи:

– практико-ориентированное обучение, позволяющее сочетать фундаментальные знания с практическими навыками по направлению подготовки 10.03.01 Информационная безопасности, учитывающие требования предъявляемых к выпускникам на рынке труда, обобщения отечественного и зарубежного опыта, проведения консультаций с ведущими работодателями и иных источников;

– формирование готовности выпускников Университета к активной профессиональной и социальной деятельности

- раскрытие места информационной безопасности и защиты информации в системе информационных отношений;

- раскрытие направлений и областей деятельности субъектов информационных отношений, составной частью которых является обеспечение информационной безопасности и защита информации;

- определение места защиты информации в обеспечении сохранности документальной базы, раскрывающей различные стороны социально-экономического и культурного развития страны.

II. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Учебная дисциплина «**Комплексное обеспечение информационной безопасности автоматизированных систем»**

относится к обязательной части программы

Для изучения данной учебной дисциплины (модуля) необходимы знания, умения и навыки, формируемые предшествующими дисциплинами*:*

«Психология социального взаимодействия, саморазвития и самоорганизации»,

«Документоведение. Нормативные документы в сфере информационной безопасности».

«Защита и обработка конфиденциальных документов», «Основы построения и функционирования технических средств защиты информации», «Компьютерная защита информации от несанкционированного доступа», «Управление проектами», «Защита информации от утечки по техническим каналам», «Организационное и правовое обеспечение информационной безопасности»

Перечень последующих учебных дисциплин, для которых необходимы знания, умения и навыки, формируемые данной учебной дисциплиной: «Техническая защита персональных данных», «Техническая защита объектов критической информационной инфраструктуры», «Государственная итоговая аттестация».

III. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Процесс освоения дисциплины направлен на формирование компетенций в соответствии с ФГОС ВО и ОП ВО по данному направлению подготовки (специальности**) 10.03.01 Информационная безопасность**

Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций

Компетенция	Индикаторы компетенций	Результаты обучения
ПК-2. Способен проводить контроль защищенности информации от утечки за счет побочных электромагнитных излучений и наводок.	ИДК$_{ПК2.1}$ Проводит контроль защищенности информации от утечки за счет побочных электромагнитных излучений и наводок.	**Знать:** методику защищенности информации от утечки за счет побочных электромагнитных излучений и наводок; **Уметь:** применять методику защищенности информации от утечки за счет побочных электромагнитных излучений и наводок; **Владеть:** навыками по применению методики защищенности информации от утечки за счет побочных электромагнитных излучений и наводок.
	ИДК$_{ПК2.2}$ Выбирает методики исследования на побочные электромагнитные излучения и наводок технических средств обработки информации	**Знать:** методики исследования на побочные электромагнитные излучения и наводок технических средств обработки информации **Уметь:** выбирать методики исследования на побочные электромагнитные излучения и наводок технических средств обработки информации **Владеть:** методиками исследования на побочные электромагнитные излучения и

		наводок технических средств обработки информации
ПК-3. Способен проводить контроль защищенности акустической речевой информации от утечки по техническим каналам	$ИДК_{ПК3.1}$ Проводит контроль защищенности акустической речевой информации от утечки по техническим каналам	**Знать:** технологию защищенности акустической речевой информации от утечки по техническим каналам **Уметь:** выбирать методики защищенности акустической речевой информации от утечки по техническим каналам **Владеть:** методиками защищенности акустической речевой информации от утечки по техническим каналам
	$ИДК_{ПК3.2}$ Выбирает методики контроля защищенности акустической речевой информации от утечки по техническим каналам	**Знать:** методики контроля защищенности акустической речевой информации от утечки по техническим каналам **Уметь:** выбирать методики контроля защищенности акустической речевой информации от утечки по техническим каналам **Владеть:** методиками контроля защищенности акустической речевой информации от утечки по техническим каналам

IV. СОДЕРЖАНИЕ И СТРУКТУРА ДИСЦИПЛИНЫ

Объем дисциплины составляет 5 зачетных единиц, 180 часов,

Из них реализуется с использованием электронного обучения и дистанционных образовательных технологий 26 часов

Из них 13 часов – практическая подготовка

Форма промежуточной аттестации: зачет

4.1 Содержание дисциплины, структурированное по темам, с указанием видов учебных занятий и отведенного на них количества академических часов

№ п/н	Раздел дисциплины/тема	Семестр	Всего часов	Из них практическая подготовка обучающихся	Виды учебной работы, включая самостоятельную работу обучающихся , практическую подготовку и трудоемкость (в часах)				Форма текущего контроля успеваемости/ Форма промежуточной аттестации (по семестрам)
					Контактная работа преподавателя с обучающимися			Самостоятельная работа	
					Лекция	Семинар/ Практическое, лабораторное занятие/	Консультация		
1	2	3	4	5	6	7	8	9	10
1	**1.Автоматизированная система**	8			4			2	собеседование
2	**2.Нормативно – правовое регулирование деятельности в области защиты информации в РФ**	8							собеседование

3	Организационно-технические методы ЗИ	**8**			4			4	собеседование
4	Нормативно-методические документы ФСТЭК России	**8**				2			собеседование
5	Выбор методов и способов защиты информации. Методы и способы защиты информации от НСД	**8**			4			4	собеседование
6	Методы и способы защиты информации от утечки по ТКУИ	**8**				2			тестирование
7	Основные вопросы управления обеспечением безопасности	**8**			4			4	собеседование
8	Создание системы защиты конфиденциальной информации (КИ)	**8**				2			собеседование
9	Предпроектное обследование СЗ (КИ) Техническое задания на разработку СЗ (КИ)	**8**			4			6	собеседование
11	Структура информационной системы Наличие подключений к сетям связи общего пользования и (или) сетям международного информационного обмена	**8**			4				тестирование
12	**3.Угрозы несанкционированного доступа к информации**	**8**							собеседование
13	Угрозы доступа в операционную среду компьютера с использованием штатного программного обеспечения	**8**				4			собеседование
14	Угрозы создания нештатных режимов работы программных (программно-аппаратных) средств	**8**			4			5	собеседование
15	Угрозы создания нештатных режимов работы программных (программно-аппаратных) средств. Угрозы внедрения вредоносных программ (программно - математического воздействия).	**8**				2		4	собеседование

	• преднамеренных изменений служебных данных; • игнорирования предусмотренных в штатных условиях ограничений на состав и характеристики обрабатываемой информации; • искажения (модификации) самих данных и т.п.;								
16	Угрозы НСД реализуемые с использованием протоколов сетевого осуществляются с использованием взаимодействия программных и программно-аппаратных средств ввода/вывода компьютера	**8**			4			4	тестирование
17	Источники угроз НСД: -нарушитель; -носитель вредоносной программы; -аппаратная закладка	**8**				2			собеседование
18	Внешние источники угроз: -разведывательные службы государств; -криминальные структуры; -конкуренты (конкурирующие организации); -недобросовестные партнеры; -внешние субъекты (физические лица)	**8**						4	собеседование
19	Внутренние источники угроз. Категории внутренних нарушителей	**8**			4				собеседование
20	Источники угроз НСД в ИС(КИ) -нарушитель -носитель вредоносной программы -аппаратная закладка -аппаратный элемент компьютера -программный контейнер	**8**				2		4	собеседование
21	Уязвимости ИС(КИ) -уязвимости системного программного							4	

	обеспечения (в том числе протоколов сетевого взаимодействия); -уязвимости прикладного программного обеспечения (в том числе средств защиты информации).								
22	Характеристика угроз непосредственного доступа в операционную среду. Классификация угроз по условиям реализации	**8**			4			4	тестирование
24	Характеристика угроз программно-математических воздействий и нетрадиционных информационных каналов. Вредоносные программы. Нетрадиционные информационные каналы.	**8**			4			4	собеседование
25	Общая характеристика результатов НСД: -нарушение конфиденциальности; -нарушению целостности (уничтожение, изменение); -нарушению доступности (блокирование)	**8**				4		4	собеседование
26	Угрозы из внешних сетей: -«Анализа сетевого трафика» с перехватом передаваемой по сети информации; -сканирование сети, выявление открытых портов и служб, открытых соединений и др.; -внедрение ложного объекта сети; -подмена доверенного объекта; -выявление паролей; -получения НСД путем подмены доверенного объекта; -«Отказ в обслуживании»; -навязывание ложного маршрута путем несанкционированного изменения маршрутно-адресных данных;	**8**						4	собеседование

	-удаленный запуск приложений; -внедрение по сети вредоносных программ								
27	**4.Защита информации. Объект информатизации. Факторы, воздействующие на информацию. ГОСТ Р 51275-2006**								
28	Субъективные факторы Объективные факторы Виды защиты информации Правовая защита информации Техническая защита информации Криптографическая защита информации Физическая защита информации	**8**			4			4	тестирование
29	**5.ОСОБЕННОСТИ РАБОТЫ С ПЕРСОНАЛОМ, ВЛАДЕЮЩИМ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИЕЙ**								
30	Персонал - основная опасность утраты конфиденциальной информации Организационные мероприятия по работе с персоналом, получающим доступ к конфиденциальной информации Методы получения ценной информации у персонала От персонала информация легко переходит к злоумышленнику по причине: Ошибочные и безответственные действия персонала	**8**				2		4	собеседование
31	Особенности приема и перевода сотрудников на работу, связанную с	**8**			4			4	собеседование

	владением конфиденциальной информацией. Подготовительные этапы процесса приема сотрудника на работу. Поиску кандидата на вновь создаваемую или вакантную должность - системный характер. Основные направления поиска кандидата								
32	Технологическая цепочка приема сотрудников, работа которых связана с владением конфиденциальной информацией, включает следующие процедуры	**8**				2		4	тестирование
33	Личные Качества, которыми должен обладать потенциальный сотрудник. Личные качества, не способствующие сохранению секретов	**8**				2			собеседование
34	Доступ персонала к конфиденциальным сведениям, документам и базам данных	**8**						4	собеседование
35	Текущая работа с персоналом, обладающим конфиденциальной информацией. Задачи обучения включают в себя изучение. Методика обучения.	**8**						4	собеседование
36	Основными формами контроля качества работы персонала, повышения ими своих профессиональных знаний, в том числе в части защиты информации,	**8**						4	тестирование
					52	26		89	

4.2. План внеаудиторной самостоятельной работы обучающихся по дисциплине

Семестр	Название раздела, темы	Самостоятельная работа обучающихся			Оценочное средство	Учебно-методическое обеспечение самостоятельной работы
		Вид самостоятельной работы	Сроки выполнения	Трудоемкость (час.)		
8	**1.Автоматизированная система**	внеаудиторная	1-2 неделя	2	Выполнение заданий по семинарским работам	Источники 1,2 из основной литературы и 1 из дополнительной
8	**2.Нормативно – правовое регулирование деятельности в области защиты информации в РФ**					
8	Организационно-технические методы ЗИ	внеаудиторная	2-3 неделя	4	Выполнение заданий по семинарским работам	Источники 1,3 из основной литературы и 2 из дополнительной
8	Нормативно-методические документы ФСТЭК России	внеаудиторная	2-3 неделя	2	Выполнение заданий по семинарским работам	Источники 1,3 из основной литературы и 2 из дополнительной
8	Выбор методов и способов защиты информации. Методы и способы защиты информации от НСД	внеаудиторная	2-3 неделя	2	Выполнение заданий по семинарским работам	Источники 1,3 из основной литературы и 2 из дополнительной

Семестр	Название раздела, темы	Самостоятельная работа обучающихся			Оценочное средство	Учебно-методическое обеспечение самостоятельной работы
		Вид самостоятельной работы	Сроки выполнения	Трудоемкость (час.)		
8	Методы и способы защиты информации от утечки по ТКУИ	внеаудиторная	3-4 неделя	2	Выполнение заданий по семинарским работам	Источники 1,5 из основной литературы и 3 из дополнительной
8	Основные вопросы управления обеспечением безопасности	внеаудиторная	3-4 неделя	2	Выполнение заданий по семинарским работам	Источники 1,6 из основной литературы и 3 из дополнительной
8	Создание системы защиты конфиденциальной информации (КИ)	внеаудиторная	3-4 неделя	2	Выполнение заданий по семинарским работам	Источники 1,6 из основной литературы и 3 из дополнительной
8	Предпроектное обследование СЗ (КИ) Техническое задания на разработку СЗ (КИ)	внеаудиторная	5-6 неделя	2	Выполнение заданий по семинарским работам	Источники 2,1 из основной литературы и 4 из дополнительной
8	Проектирование и создание СЗ (КИ) Ввод в действие (СЗ) (КИ)	внеаудиторная	5-6 неделя	2	Выполнение заданий по семинарским работам	Источники 2,1 из основной литературы и 4 из дополнительной

Семестр	Название раздела, темы	Самостоятельная работа обучающихся			Оценочное средство	Учебно-методическое обеспечение самостоятельной работы
		Вид самостоятельной работы	Сроки выполнения	Трудоемкость (час.)		
8	Структура информационной системы Наличие подключений к сетям связи общего пользования и (или) сетям международного информационного обмена	внеаудиторная	5-6 неделя	2	Выполнение заданий по семинарским работам	Источники 2,1 из основной литературы и 4 из дополнительной
8	**3.Угрозы несанкционированного доступа к информации**					
8	Угрозы доступа в операционную среду компьютера с использованием штатного программного обеспечения	внеаудиторная	6-7 неделя	4	Выполнение заданий по семинарским работам	Источники 1-1-2-2 из основной литературы и1-4 из дополнительной
8	Угрозы создания нештатных режимов работы программных (программно-аппаратных) средств	внеаудиторная	6-7 неделя	6	Выполнение заданий по семинарским работам	Источники 2,1 из основной литературы и 2 из дополнительной
8	Угрозы НСД реализуемые с использованием протоколов сетевого осуществляются с использованием взаимодействия программных и программно-аппаратных средств ввода/вывода компьютера	внеаудиторная	7-8 неделя	6	Выполнение заданий по семинарским работам	Источники 2,1 из основной литературы и 4 из дополнительной

Семестр	Название раздела, темы	Самостоятельная работа обучающихся			Оценочное средство	Учебно-методическое обеспечение самостоятельной работы
		Вид самостоятельной работы	Сроки выполнения	Трудоемкость (час.)		
8	Внешние источники угроз: -разведывательные службы государств; -криминальные структуры; -конкуренты (конкурирующие организации); -недобросовестные партнеры; -внешние субъекты (физические лица)	внеаудиторная	7-8 неделя	4	Выполнение заданий по семинарским работам	Источники 2,1 из основной литературы и 3 из дополнительной
8	Внутренние источники угроз. Категории внутренних нарушителей	внеаудиторная	7-8 неделя	4	Выполнение заданий по семинарским работам	Источники 2,1 из основной литературы и 3 из дополнительной
8	Источники угроз НСД в ИС(КИ) -нарушитель -носитель вредоносной программы -аппаратная закладка -аппаратный элемент компьютера -программный контейнер	внеаудиторная	8-9 неделя	4	Выполнение заданий по семинарским работам	Источники 2,1 из основной литературы и 4 из дополнительной
8	Уязвимости ИС(КИ) -уязвимости системного программного обеспечения (в том числе протоколов сетевого взаимодействия); -уязвимости прикладного программного обеспечения (в том числе средств защиты информации).	внеаудиторная	8-9 неделя	4	Выполнение заданий по семинарским работам	Источники 2,1 из основной литературы и 5 из дополнительной

Семестр	Название раздела, темы	Самостоятельная работа обучающихся			Оценочное средство	Учебно-методическое обеспечение самостоятельной работы
		Вид самостоятельной работы	Сроки выполнения	Трудоемкость (час.)		
8	Характеристика угроз непосредственного доступа в операционную среду. Классификация угроз по условиям реализации	внеаудиторная	9-10 неделя	4	Выполнение заданий по семинарским работам	Источники 2,1 из основной литературы и5 из дополнительной
8	Характеристика угроз, реализуемых с использованием протоколов межсетевого взаимодействия. Классификация угроз.	внеаудиторная	9-10 неделя	4	Выполнение заданий по семинарским работам	Источники 2,1 из основной литературы и 4 из дополнительной
8	Характеристика угроз программно-математических воздействий и нетрадиционных информационных каналов. Вредоносные программы. Нетрадиционные информационные каналы.	внеаудиторная	9-10 неделя	4	Выполнение заданий по семинарским работам	Источники 2,1 из основной литературы и 4 из дополнительной
8	Общая характеристика результатов НСД: -нарушение конфиденциальности; -нарушению целостности (уничтожение, изменение); -нарушению доступности (блокирование)	внеаудиторная	10-11 неделя	4	Выполнение заданий по семинарским работам	Источники 2,1 из основной литературы и 4 из дополнительной
8	Угрозы из внешних сетей	внеаудиторная	10-11 неделя	4	Выполнение заданий по семинарским работам	Источники 2,1 из основной литературы и 4 из дополнительной

Семестр	Название раздела, темы	Самостоятельная работа обучающихся			Оценочное средство	Учебно-методическое обеспечение самостоятельной работы
		Вид самостоятельной работы	Сроки выполнения	Трудоемкость (час.)		
8	**4.Защита информации. Объект информатизации. Факторы, воздействующие на информацию. ГОСТ Р 51275-2006**					
8	Субъективные факторы Объективные факторы Виды защиты информации Правовая защита информации Техническая защита информации Криптографическая защита информации Физическая защита информации	внеаудиторная	11-12 неделя	4	Выполнение заданий по семинарским работам	Источники 2,1 из основной литературы и 4 из дополнительной
8	**5.ОСОБЕННОСТИ РАБОТЫ С ПЕРСОНАЛОМ, ВЛАДЕЮЩИМ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИЕЙ**					
8	Персонал - основная опасность утраты конфиденциальной информации Организационные мероприятия по работе с персоналом, получающим доступ к конфиденциальной информации	внеаудиторная	12-13 неделя	4	Выполнение заданий по семинарским работам	Источники 2,1 из основной литературы и 4 из дополнительной

Семестр	Название раздела, темы	Самостоятельная работа обучающихся			Оценочное средство	Учебно-методическое обеспечение самостоятельной работы
		Вид самостоятельной работы	Сроки выполнения	Трудоемкость (час.)		
8	Особенности приема и перевода сотрудников на работу, связанную с владением конфиденциальной информацией.	внеаудиторная	13-14 неделя	4	Выполнение заданий по семинарским работам	Источники 2,1 из основной литературы и 4 из дополнительной
8	Технологическая цепочка приема сотрудников, работа которых связана с владением конфиденциальной информацией, включает следующие процедуры	внеаудиторная	14-15 неделя	4	Выполнение заданий по семинарским работам	Источники 2,1 из основной литературы и 4 из дополнительной
8	Текущая работа с персоналом, обладающим конфиденциальной информацией. Задачи обучения включают в себя изучение. Методика обучения.	внеаудиторная	15-16 неделя	4	Выполнение заданий по семинарским работам	Источники 2,1 из основной литературы и 4 из дополнительной
8	Основными формами контроля качества работы персонала, повышения ими своих профессиональных знаний, в том числе в части защиты информации,	внеаудиторная	16-17 неделя	4	Выполнение заданий по семинарским работам	Источники 2,1 из основной литературы и 4 из дополнительной
Общий объем самостоятельной работы по дисциплине (час)				**89**		
Из них объем самостоятельной работы **с использованием электронного обучения и дистанционных образовательных технологий (час)**				**20**		

4.3.Содержание учебного материала

4.3.1. Перечень семинарских, практических занятий и лабораторных работ

4.3.5 Перечень семинарских, практических занятий и лабораторных работ

№ п/н	№ раздела и темы	Наименование семинаров, практических и лабораторных работ	Трудоемкость (час.)		Оценочные средства	Формируемые компетенции (индикаторы) *
			Всего часов	Из них практическая подготовка		
1	2	3	4	5	6	7
1	1	Нормативно-методические документы ФСТЭК России	2	2	Выполнение заданий по вопросам семинара	$ИДК_{ПК2.1.}$
2	2	Методы и способы защиты информации от утечки по ТКУИ	2	2	Выполнение заданий по вопросам семинара	$ИДК_{ПК2.1.}$
3	2	Создание системы защиты конфиденциальной информации (КИ)	2	2	Выполнение заданий по вопросам семинара	$ИДК_{ПК2.2}$
4	3	Угрозы доступа в операционную среду компьютера с использованием штатного программного обеспечения	4	4	Выполнение заданий по вопросам семинара	$ИДК_{ПК2.2}$
5	3	Угрозы создания нештатных режимов работы программных (программно-аппаратных) средств.	2	2	Выполнение заданий по вопросам семинара	$ИДК_{ПК2.2}$
6	3	Источники угроз НСД	2	2	Выполнение заданий по вопросам семинара	$ИДК_{ПК2.2}$
7	3	Общая характеристика результатов НСД	4	4	Выполнение заданий по вопросам семинара	$ИДК_{ПК2.2}$

8	4	Организационные мероприятия по работе с персоналом, получающим доступ к конфиденциальной информации	2	2	Выполнение заданий по вопросам семинара	$ИДК_{ПК3.1}$
9	4	Технологическая цепочка приема сотрудников, работа которых связана с владением конфиденциальной информацией, включает следующие процедуры	2	2	Выполнение заданий по вопросам семинара	$ИДК_{ПК3.2}$

4.3.2. Перечень тем (вопросов), выносимых на самостоятельное изучение студентами в рамках самостоятельной работы (СРС)

№ п/п	Тема	Задание	Формируемая компетенция	ИДК
1	**2**	**3**	**4**	**5**
1	Организационно-технические методы ЗИ	Подготовка по вопросам семинара	ПК-1	$ИДК_{ПК1.1}$
2	Нормативно-методические документы ФСТЭК России	Подготовка по вопросам семинара	ПК-1	$ИДК_{ПК1.2}$
3	Выбор методов и способов защиты информации. Методы и способы защиты информации от НСД	Подготовка по вопросам семинара	ПК-2	$ИДК_{ПК2.1}$
4	Методы и способы защиты информации от утечки по ТКУИ	Подготовка по вопросам семинара	ПК-2	$ИДК_{ПК2.1}$
5	Основные вопросы управления обеспечением безопасности	Подготовка по вопросам семинара	ПК-2	$ИДК_{ПК2.2}$
6	Создание системы защиты конфиденциальной информации (КИ)	Подготовка по вопросам семинара	ПК-2	$ИДК_{ПК2.2}$
7	Предпроектное обследование СЗ (КИ) Техническое задания на разработку СЗ (КИ)	Подготовка по вопросам семинара	ПК-2	$ИДК_{ПК2.2}$

8	Проектирование и создание СЗ (КИ) Ввод в действие (СЗ) (КИ)	Подготовка по вопросам семинара	ПК-2	ИДК$_{ПК2.2}$
9	Структура информационной системы Наличие подключений к сетям связи общего пользования и (или) сетям международного информационного обмена	Подготовка по вопросам семинара	ПК-2	ИДК$_{ПК2.2}$
10	**3.Угрозы несанкционированного доступа к информации**			
11	Угрозы доступа в операционную среду компьютера с использованием штатного программного обеспечения	Подготовка по вопросам семинара	ПК-3	ИДК$_{ПК3.1}$
12	Угрозы создания нештатных режимов работы программных (программно-аппаратных) средств	Подготовка по вопросам семинара	ПК-3	ИДК$_{ПК3.1}$
13	Угрозы НСД реализуемые с использованием протоколов сетевого осуществляются с использованием взаимодействия программных и программно-аппаратных средств ввода/вывода компьютера	Подготовка по вопросам семинара	ПК-3	ИДК$_{ПК3.1}$
14	Внешние источники угроз: -разведывательные службы государств; -криминальные структуры; -конкуренты (конкурирующие организации); -недобросовестные партнеры; -внешние субъекты (физические лица)	Подготовка по вопросам семинара	ПК-3	ИДК$_{ПК3.1}$
15	Внутренние источники угроз. Категории внутренних нарушителей	Подготовка по вопросам семинара	ПК-3	ИДК$_{ПК3.1}$
16	Источники угроз НСД в ИС(КИ) -нарушитель -носитель вредоносной программы -аппаратная закладка	Подготовка по вопросам семинара	ПК-3	ИДК$_{ПК3.1}$

	-аппаратный элемент компьютера -программный контейнер			
17	Уязвимости ИС(КИ) -уязвимости системного программного обеспечения (в том числе протоколов сетевого взаимодействия); -уязвимости прикладного программного обеспечения (в том числе средств защиты информации).	Подготовка по вопросам семинара	ПК-3	$ИДК_{ПК3.1}$
18	Характеристика угроз непосредственного доступа в операционную среду. Классификация угроз по условиям реализации	Подготовка по вопросам семинара	ПК-3	$ИДК_{ПК3.1}$
19	Характеристика угроз, реализуемых с использованием протоколов межсетевого взаимодействия. Классификация угроз.	Подготовка по вопросам семинара	ПК-3	$ИДК_{ПК3.1}$
20	Характеристика угроз программно-математических воздействий и нетрадиционных информационных каналов. Вредоносные программы. Нетрадиционные информационные каналы.	Подготовка по вопросам семинара	ПК-3	$ИДК_{ПК3.1}$
21	Общая характеристика результатов НСД: -нарушение конфиденциальности; -нарушению целостности (уничтожение, изменение); -нарушению доступности (блокирование)	Подготовка по вопросам семинара	ПК-3	$ИДК_{ПК3.1}$
22	Угрозы из внешних сетей	Подготовка по вопросам семинара	ПК-3	$ИДК_{ПК3.1}$
23	**4.Защита информации. Объект информатизации. Факторы, воздействующие на информацию. ГОСТ Р 51275-2006**			
24	Субъективные факторы Объективные факторы Виды защиты информации	Подготовка по вопросам семинара	ПК-3	$ИДК_{ПК3.2}$

	Правовая защита информации Техническая защита информации Криптографическая защита информации Физическая защита информации			
25	**5.ОСОБЕННОСТИ РАБОТЫ С ПЕРСОНАЛОМ, ВЛАДЕЮЩИМ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИЕЙ**			
26	Персонал - основная опасность утраты конфиденциальной информации Организационные мероприятия по работе с персоналом, получающим доступ к конфиденциальной информации	Подготовка по вопросам семинара	ПК-3	ИДК$_{ПК3.2}$
27	Особенности приема и перевода сотрудников на работу, связанную с владением конфиденциальной информацией.	Подготовка по вопросам семинара	ПК-3	ИДК$_{ПК3.2}$
28	Технологическая цепочка приема сотрудников, работа которых связана с владением конфиденциальной информацией, включает следующие процедуры	Подготовка по вопросам семинара	ПК-3	ИДК$_{ПК3.2}$
29	Текущая работа с персоналом, обладающим конфиденциальной информацией. Задачи обучения включают в себя изучение. Методика обучения.	Подготовка по вопросам семинара	ПК-3	ИДК$_{ПК3.2}$
30	Основными формами контроля качества работы персонала, повышения ими своих профессиональных знаний, в том числе в части защиты информации,	Подготовка по вопросам семинара	ПК-3	ИДК$_{ПК3.2}$

4.4. Методические указания по организации самостоятельной работы студентов

а) Методические рекомендации по изучению теоретической части учебного модуля

Теоретические занятия дисциплины представлены в виде лекций.

Цель лекции – организация целенаправленной познавательной деятельности студентов по овладению программным материалом дисциплины.

Задачи лекционных занятий – дать связанное, последовательное изложение материала, сообщить студентам основное содержание предмета в целостном, систематизированном виде.

Структура и содержание основных разделов **(**приведена в рабочей программе учебной дисциплины, раздел 4.1)

Методы и средства проведения теоретических занятий

При изучении учебного модуля студенты должны посещать лекционные занятия, вести конспекты и самостоятельно прорабатывать по учебникам вопросы, указанные преподавателем. (Список основной литературы приведен разделе 5).

Отличительной особенностью данной дисциплины является ее практическая направленность. В ходе лекций предполагается рассматривать только основные теоретические вопросы защиты информации, а подробное изучение теоретических положений и практических приложений теории, а также получение навыков работы в современных информационных системах защиты информации на языке программирования высокого уровня должно проводиться в часы семинарских занятий, а также внеаудиторной СРС. Для этого преподаватель выдает студентам задания по вопросам на семинарских занятиях.

б) Методические рекомендации по самостоятельной работе студентов

Аудиторная самостоятельная работа студентов заключается в выполнении одной контрольной реферативной работы в середине семестра и сдаче итогового экзаменационного теста для получения оценки. Внеаудиторная самостоятельная работа студентов заключается в подготовке к лекционным занятиям, подготовке к выполнению семинарских заданий. Самостоятельная работа подразумевает систематический подход к обучению, в соответствии с предложенным в разделе 4.2 графиком, что, в свою очередь, способствует успешной подготовке к зачету.

4.5. Примерная тематика курсовых работ

Выполнение курсовых работ не предусмотрено учебным планом

4.3.7. Методические указания по организации самостоятельной работы студентов

а) Методические рекомендации по изучению теоретической части учебного модуля

Теоретические занятия дисциплины представлены в виде лекций.

Цель лекции – организация целенаправленной познавательной деятельности студентов по овладению программным материалом дисциплины.

Задачи лекционных занятий – дать связанное, последовательное изложение материала, сообщить студентам основное содержание предмета в целостном, систематизированном виде.

Структура и содержание основных разделов **(**приведена в рабочей программе учебной дисциплины, раздел 4.1)

Методы и средства проведения теоретических занятий

При изучении учебного модуля студенты должны посещать лекционные занятия, вести конспекты и самостоятельно прорабатывать по учебникам вопросы, указанные преподавателем. (Список основной литературы приведен разделе 5).

Отличительной особенностью данной дисциплины является ее практическая направленность. В ходе лекций предполагается рассматривать только основные теоретические вопросы защиты информации, а подробное изучение теоретических положений и практических приложений теории, а также получение навыков работы в современных информационных системах защиты информации на языке программирования высокого уровня должно проводиться в часы семинарских занятий, а также внеаудиторной СРС. Для этого преподаватель выдает студентам задания по вопросам на семинарских занятиях.

б) Методические рекомендации по самостоятельной работе студентов

Аудиторная самостоятельная работа студентов заключается в выполнении одной контрольной реферативной работы в середине семестра и сдаче итогового экзаменационного теста для получения оценки. Внеаудиторная самостоятельная работа студентов заключается в подготовке к лекционным занятиям, подготовке к выполнению семинарских заданий. Самостоятельная работа подразумевает систематический подход к обучению, в соответствии с предложенным в разделе 4.2 графиком, что, в свою очередь, способствует успешной подготовке к зачету.

4.3.8 Примерная тематика курсовых работ (проектов) *(указать при наличии)*

По учебному плану - отсутствует

5 УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ				
5.1 Учебная литература				
5.1.1 Основная литература				
	Авторы, составители	Заглавие	Издательство, год издания	Кол-во экз. в библиотеке/ 100% онлайн
Л1.1	В.Я.Ищейнов.	Защита конфиденциальной информации: учебное пособие	Изд. Фррум,М 2015. – 146 с.	25
Л1.2	М. В. Гришина	Комплексная система защиты информации на предприятии: учебное пособие	Изд. Фррум,М 2009. - 2009	18
Л1.3	О.В. Прохорова	Информационная безопасность и защита информации: Учебник [Электронный ресурс] //biblioclub.ru/index.php?page=book&id=438331	Самара: СГА-СУ, 2014	100% Онлайн
Л14	М.А. Лапина, А.Г. Ревин, В.И. Лапин	Информационное право : учебное пособие [Электронный ресурс] //biblioclub.ru/index.php?page=book&id=118624	М. : Юнити-Дана, 2015	100% Онлайн
5.1.2 Дополнительная литература				
	Авторы, составители	Заглавие	Издательство, год издания	Кол-во экз. в библиотеке/ 100% онлайн
Л2.1	Ю.Н. Загинайлов	Теория информационной безопасности и методология защиты информации: учебное пособие //biblioclub.ru/index.php?page=book&id=276557	М. ; Берлин : Директ-Медиа, 2015	100% онлайн

Л2.2	О.В. Прохорова	Информационная безопасность и защита информации: Учебник [Электронный ресурс] //biblioclub.ru/index.php?page=book&id=438331	Самара: СГА-СУ, 2014	100% онлайн
Л2.3	Коваленко, Ю.И	Правовой режим лицензирования и сертификации в сфере информационной безопасности: Учебные пособия [Электронный ресурс] http://e.lanbook.com/book/5163	М. : Горячая линия-Телеком, 2012	100% Онлайн
5.1.3 Методические разработки				
	Авторы, составители	Заглавие	Издательство, год издания/ Личный кабинет обучающегося	Кол-во экз. в библиотеке/ 100% онлайн
Л3.1	Глухов Н.И.	Оценка информационных рисков предприятия: учеб. пособие/ Н. И. Глухов; Федер. агентство ж.-д. трансп., Иркут. гос. ун-т путей сообщ... - 148 с	- Иркутск: ИрГУПС, 2013	55
5.1.4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине				
	Авторы, составители	Заглавие	Издательство, год издания/ Личный кабинет обучающегося	Кол-во экз. в библиотеке/ 100% онлайн
Л4.1	Глухов Н.И.	Материалы для самостоятельной работы студентов	Личный кабинет студента	100% онлайн
5.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет»				
Э.1	Линия защиты «Сюртель» www.suritel.ru			
Э.2	Федеральная служба по техническому и экспортному контролю, www.fstec.ru			
5.3 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем				
5.3.1 Перечень базового программного обеспечения				
6.3.1.1	ОС Microsoft Windows 7 Professional, лицензия № 49379844, обновление - контракт №0334100010018000027-0000756-02 от 28.05.2018 АО СофтЛайн Трейд, обновление - контракт № 0334100010019000029-0000756-02 от 17.09.2019г. АО СофтЛайн Трейд, контракт № 0334100010020000010-0000756-02 от 16.06.2020 АО СофтЛайн Трейд Windows Edu Per Device 10 Education, Соглашение № V6760694, обновление - контракт № 0334100010020000010-0000756-02 от 16.06.2020 АО СофтЛайн Трейд		
6.3.1.2	Офисный пакет Microsoft Office 2010, Лицензия № 48288083, обновление - контракт №0334100010018000027-0000756-02 от 28.05.2018 АО СофтЛайн Трейд, обновление - контракт № 0334100010019000029-0000756-02 от 17.09.2019г. АО СофтЛайн Трейд, обновление - контракт № 0334100010020000010-0000756-02 от 16.06.2020 АО СофтЛайн Трейд; Office Professional 2019 - Соглашение № V0709762, контракт № 0334100010020000010-0000756-02 от 16.06.2020 АО СофтЛайн Трейд; LibreOffice v. 5.2, свободно распространяемое ПО, https://ru.libreoffice.org		
5.3.2 Перечень специализированного программного обеспечения				
6.3.2.1	Microsoft PowerPoint Viewer 2007, бесплатно, количество не ограничено.			
5.3.3 Перечень информационных справочных систем				
6.3.3.1	«Консультант +» http://www.consultant.ru/			
6.3.3.2	«Техэксперт» http://www.cntd.ru/			
5.4 Перечень правовых и нормативных документов				
6.4.1	Не предусмотрено			

VI. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Учебно-лабораторное оборудование:

Офисное оборудование для оперативного размножения иллюстративного и раздаточного лекционного материала.

6.2. Программное обеспечение:

Интегрированная среда разработки ПО Microsoft Visual Studio (2019 Community).

6.3. Технические и электронные средства:

В ходе учебного процесса используются технические средства обучения и контроля знаний студентов (презентации, контролирующих программ, демонстрационных установок), использование которых предусмотрено методической концепцией преподавания

VII.ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Чтение лекций по темам предполагает разбор конкретных ситуаций в качестве примеров, подкрепляющих теоретический материал.

При проведении лабораторных занятий студентам (в отдельных случая – группам студентов) предлагается выполнение разнообразных творческих заданий по текущей теме.

VIII. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Материалы для проведения текущего и промежуточного контроля знаний студентов:

Для оценки достижений студентов в процессе изучения дисциплины; управления процессом приобретения студентами необходимых знаний, умений, навыков и формирования компетенций; оценки способностей студента к творческой деятельности, обеспечивающей решения новых задач; обеспечения соответствия результатов обучения задачам будущей профессиональной деятельности осуществляется поэтапный контроль степени освоения компетенций. В таблице приведены этапы освоения компетенций и виды оценочных средств, предназначенных для оценивания компетенций на разных стадиях обучения студентов.

№ п/п	Модуль, раздел (в соответствии с РП)	Контролируемые компетенции (или их части)	Вид оценочного средства
1	Раздел 1	ПК-1	Зачет по теме
2	Раздел 2	ПК-2	Зачет по теме
3	Раздел 3	ПК-3	Зачет по теме
4	Раздел 4	ПК-3	Тестирование

Контроль качества освоения студентами дисциплины осуществляется непрерывно в течение всего периода обучения с использованием балльно-рейтинговой системы (БРС). Индикатором сформированности компетенции является начисление студенту баллов за выполнение задания семинаров, контрольных работ в виде теста, получения премиальных баллов и /или выполнения итогового теста.

Назначение оценочных средств текущего контроля – выявить сформированность компетенций (ПК-2,ПК-3). Ниже приведен перечень оценочных средств текущего контроля:

Тест

1 «Информация» это:

а совокупность содержащихся в базах данных сведений

б совокупность содержащихся в базах данных сведений, зафиксированных на машин-ных носителях

в сведения (сообщения, данные) воспроизводимые различными системами

г сведения (сообщения, данные) независимо от формы их представления

2 «Информационная система» это:

а совокупность информации, информационных технологий и технических средств

б совокупность информации, информационных технологий, технических средств и персонала, обслуживающего систему

в совокупность информационных технологий и технических средств

г совокупность информации, технических средств и персонала, обслуживающего ин-формационную систему

д совокупность информации, технических средств и персонала, обслуживающего и эксплуатирующего информационную систему

3 Одним из основных факторов учитываемых при выборе средств антивирусной защиты является:

а удобство эксплуатации

б совместимость со штатным ПО

в наличие графического интерфейса

г Быстродействие

4 «Обладатель информации» это:

а лицо, самостоятельно создавшее информацию

б лицо получившее на основании закона или договора право разрешать или ограничивать доступ к информации

в лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам

г лицо, самостоятельно создавшее информацию либо получившее право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам

5 «Предоставление информации» это:

а действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц

б действия, направленные на распространение сведений в средствах массовой информации

в действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц

г действия, направленные на получение информации как определённым так и неопределённым кругом лиц или передачу информации как определенному так и неопределённому кругу лиц

6 «Защищаемые помещения» это:

а помещения, специально предназначенные для хранения носителей конфиденциальной информации

б помещения, специально предназначенные для размещения технических средств информационной системы

в помещения, специально предназначенные для хранения носителей конфиденциальной информации и размещения технических средств информационной системы

г помещения, специально предназначенные для проведения конфиденциальных мероприятий

7 «Контролируемая зона» это:

а пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств

б часть здания, в котором исключено неконтролируемое пребывание посторонних лиц, транспортных, технических и иных материальных средств

в пространство (территория, здание, часть здания, помещение), в котором действует особый режим наблюдения за всеми сотрудниками организации

г помещение, в котором постоянно, независимо от окружающих факторов ведётся систематический контроль и надзор за действиями пользователей

8 К рекомендуемым методам и способам защиты информации в информационных системах относятся (выберите все верные варианты ответов)

а методы и способы защиты информации от несанкционированного доступа

б методы и способы сокрытия информации от внутренних нарушителей

в методы и способы устранения конкурентов

г методы и способы защиты информации от утечки по техническим каналам

9 Документом, определяющим лицензируемые виды деятельности, является:

а Постановление правительства РФ от 26 января 2006 г. № 45
Об организации лицензирования отдельных видов деятельности

б Постановление Правительство РФ от 15 августа 2006 г. № 504
О лицензировании деятельности по технической защите конфиденциальной инфор-мации

в Постановление Правительства РФ от 31 августа 2006 г. № 532
О лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации

г ФЗ “О лицензировании отдельных видов деятельности” 99-ФЗ от 4 мая 2011 г.

д ФЗ “О техническом регулировании” 184-ФЗ от 27 декабря 2002 г.

10 Средствами защиты информации, подлежащими сертификации являются:
(выберите все верные варианты ответов)

а строительные материалы, используемые для отделки помещений в которых размещаются отдельные элементы ИСПДн

б детали интерьера, используемые для размещения ИСПДн

в средства контроля эффективности применения средств защиты информации

г средства контроля эффективности прочности ограждений

д средства защиты информации (технические, программные, программно-технические) от НСД, блокировки доступа и нарушения целостности

11 Программное обеспечение средств защиты информации, каких классов ИСПДн должно проходить контроль отсутствия недекларированных возможностей (НДВ)?

а К1

б К2

в К3

г К4

12 Технические способы защиты информации в зависимости от используемых средств классифицируются как: (выберите все верные варианты ответов)

а Полуактивные

б Пассивные

в Разноплановые

г Удостоверяющие

д Активные

13 По заданным оператором характеристикам безопасности персональных данных, обрабатываемых в информационной системе, ИСПДн подразделяются на:
(выберите все верные варианты ответов)

а Автоматизированные

б типовые
в Неавтоматизированные
г Специальные
д Специализированные
е Комбинированные

14 “Технический канал утечки информации” это:

а совокупность объекта технической разведки, физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация

б совокупность средств доступа к информации, нарушающих правила разграничения доступа с использованием штатных средств

в совокупность физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация

г совокупность объекта технической разведки и средств, которыми добывается защищаемая информация

15 Техническими каналами утечки информации, приводящими к возникновению угроз безопасности персональных данных являются:
(выберите все верные варианты ответов)

а кражи технических средств информационной системы
б утечки акустической (речевой) информации
в утечки информации реализуемые через общедоступные информационные сети
г утечки видовой информации
д утечки информации по каналам побочных электромагнитных излучений
е утечки информации реализуемые через интернет

16 “Несанкционированный доступ” (НСД) к информации” это:

а доступ, реализующий возможности совокупности физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация

б доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств

в доступ с использованием совокупности средств технической разведки и прочих средств, которыми добывается защищаемая информация

г доступ к информации, реализуемый путём уничтожения технических средств информационной системы

17 Выберите информационные системы, в которых требуется обеспечение только конфиденциальности персональных данных:

а Автоматизированные
б типовые
в Неавтоматизированные
г Специальные
д Специализированные

18 “Специальные исследования (специсследования)” это:

а выявление с помощью контрольно - измерительной аппаратуры возможных каналов утечки информации

б определение соответствия условий эксплуатации объектов информатизации требованиям аттестатов соответствия, и других руководящих документов по спецзащите без применения контрольно - измерительной аппаратуры

в проверки технических средств иностранного и совместного производства на наличие возможно внедренных электронных устройств перехвата информации.

19 Пассивными способами защиты информации являются:

а создание маскирующих электромагнитных помех в посторонних проводниках и соединительных линиях технических средств.

б ослабление наводок ПЭМИ в посторонних проводниках и соединительных линиях технических средств, выходящих за пределы контролируемой зоны.

в создание маскирующих электромагнитных помех в цепях заземления ИСПДн.

г выставление постов охраны у помещений в которых размещаются технические средства обработки информации

20 Количество категорий внутренних нарушителей для ИСПДн, определяемых нормативными документами ФСТЭК:

а 4

б 5

в 6

г 7

д 8

е 9

21 Активными способами защиты информации являются:

а Ослабление проникновения информационных сигналов в цепи электропитания аппаратных средств ИСПДн, выходящие за пределы контролируемой зоны.

б Создание маскирующих электромагнитных помех в посторонних проводниках и соединительных линиях технических средств.

в Ослабление ПЭМИ.

г Правильная разработка организационно-распорядительной документации для обеспечения информационной безопасности.

22 Рекомендуемые стадии создания системы защиты информации:
(выберите все верные варианты ответов)

а Экспериментальная

б ввода в действие

в Согласования

г проектирования и реализации

д Предпроектная

е Утверждения

23 Обязательной аттестации по требованиям безопасности информации подлежат информационные системы персональных данных следующих классов:

а К 1 и К 2

б К 2 и К 3

в Только К 1

г Только К 2

д Только К 3

е Требования не предъявляются

24 К специальным ИСПДн могут быть отнесены информационные системы, в которых:
(выберите все верные варианты ответов)

а требуется обеспечить специальную охрану

б требуется обеспечить конфиденциальность и целостность информации

в требуется обеспечить только конфиденциальность информации

г требуется обеспечить хотя бы одну из характеристик безопасности, отличную от конфиденциальности

25 Условием доработки функционирующих информационных систем является:

а смена руководства организации

б смена администратора, ответственного за защиту информации

в изменение класса информационной системы

г изменение погодных условий

26 Ко второй категории обрабатываемых персональных данных относятся:

а обезличенные и (или) общедоступные персональные данные

б расовая, национальная принадлежность, политические взгляды, религиозные и философские убеждения, состояние здоровья и интимной жизни

в данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию

г данные, позволяющие идентифицировать субъекта персональных данных

27 Методами и способами защиты информации от несанкционированного доступа являются: (выберите все верные варианты ответов)

а учет и хранение съемных носителей информации

б использование средств линейного электромагнитного зашумления

в размещение объектов защиты в соответствии с предписанием на эксплуатацию

г использование сертифицированных средств защиты информации

д звукоизоляция ограждающих конструкций

е организация физической защиты помещений

28 Сопротивления заземляющих проводников, а также земляных шин должны быть:

а более 8 Ом

б не более 8 Ом

в более 6 Ом

г не более 6 Ом

д более 4 Ом

е не более 4 Ом

29 Рекомендуемым условием применения линейного электромагнитного зашумления является:

а питание ИСПДн осуществляется от трансформаторной подстанции, расположенной в пределах контролируемой зоны

б обеспечивается требуемый пространственный разнос аппаратных средств ИСПДн и их соединительных линий или посторонних проводников, имеющих выход за пределы контролируемой зоны

в к системе заземления ИСПДн возможно подключение потребителей, расположенных вне контролируемой зоны

г достаточный уровень коэффициента затухания информационного сигнала

30 При оборудовании системы электропитания ИСПДн рекомендуется:
(выберите все верные варианты ответов)

а питание от подстанции, расположенной в пределах КЗ

б питание от подстанции, расположенной за пределами КЗ

в организация ночного патрулирования вокруг трансформаторной подстанции от которой запитывается ИСПДн

г отсутствие подключения к трансформаторной подстанции, от которой запитывается ИСПДн, посторонних потребителей, расположенных за пределами контролируемой зоны

31* Какой из показателей рекомендуется учитывать при размещении технических средств внутри объекта?

а Зона 1

б Зона 2

в Зона 3

г Зона 4

д Зона 5

32* Какой из показателей рекомендуется учитывать при размещении технических средств внутри контролируемой зоны?

а Зона 1

б Зона 2

в Зона 3

г Зона 4
д Зона 5

33* Информация в зависимости от категории доступа к ней подразделяется на: (выберите все верные варианты ответов)

а Конфиденциальную
б Общедоступную
в особо конфиденциальную
г ограниченного доступа
д широкого доступа

34* Подключение информационных систем, обрабатывающих служебную тайну к сети Интернет:

а Не допускается
б Допускается
в Допускается только с использованием специально предназначенных для этого средств защиты информации
г Допускается только с использованием средств защиты информации известных производителей

35* Специальные категории персональных данных это: (выберите все верные варианты ответов)

а национальная принадлежность
б территориальное размещение
в состояние аппетита
г сверхъестественные способности
д состояние интимной жизни
е политические взгляды

36* Классами защищённости автоматизированных систем от несанкционированного доступа являются: (выберите все верные варианты ответов)

а 1Е
b 2Г
в 2А
г 2В
д 3С
е 3Б

37* Определите класс автоматизированной системы по следующим классификационным признакам: АС, в которой работает один пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности, обрабатывается “Служебная тайна”.

а 2Б
б 2А
в 1Г
г 1Д
д 3А
е 3Б

38* Определите класс автоматизированной системы по следующим классификационным признакам: многопользовательская АС, в которой одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности. И все пользователи имеют равные права доступа ко всей информации АС, обрабатывается “Служебная тайна” и общедоступная информация.

а 2Б
б 2А
в 1Г
г 1Д

д 3А
е 3Б

39* Основными элементами ИСПДн являются:
(выберите все верные варианты ответов)

а помещения для размещения технических средств
б персональные данные, содержащиеся в базах данных
в контролируемая зона
г информационные технологии
д обслуживающий персонал
е технические средства обработки информации
ж ограждающие конструкции
з технические средства перевозки материальных носителей информации

40* Источниками угроз несанкционированного доступа являются:
(выберите все верные варианты ответов)

а Нарушители
б природные факторы
в носители вредоносных программ
г аппаратные закладки
д отказы оборудования
е отказы программного обеспечения

Семинарские задания. Назначение оценочного средства – мониторинг эффективности подготовки студентов в ходе обучения. Показателем эффективности подготовки студента является получение им балла, превышающего пороговое значение в 3 балла за выполнение и усвоение одного семинарского задания. В семестре предполагается выполнение 14 семинаров. Суммарно для допуска к зачету студент должен получить за уяснение вопросов семинаров не менее 42 бала.

Параметры оценочного средства

Критерии оценки	Оценка		
	Отлично	Хорошо	Удовлетв.
Выполнение заданий	Полностью и корректно выполнены все задания **(9-10 баллов)**	Полностью выполнены все задания, допущены одна – две ошибки **(7 -8 баллов)**	Не полностью выполнены задания, допущены одна – две ошибки **(5 -6 балла)**

Промежуточная аттестация проводится в форме защиты реферата. Студент допускается к итоговой аттестации - экзамену в том случае, если он защитит реферат, выполнит все семинарские задания и получит более 42 баллов, а также сдаст на положительную оценку контрольные работы в виде тестов. Если студент набрал необходимое количество баллов, предлагается итоговый тест – экзамен.

В случае если студент не набрал пороговое значение баллов, ему предлагается пройти итоговое тестирование по тем разделам, которые остались не изучены (пропущены, не сданы на положительную оценку). Характеристики итогового теста сходны с характеристиками тестов для контрольных аттестационных работ.

Объем теста –40 вопросов.

Параметры оценочного средства

Предел длительности контроля	45 мин
Последовательность выборки вопросов из	случайная

разделов (по всему курсу дисциплины)	
Критерии оценки:	
«5», если	45 – 50 правильных ответов (добавляется 17 - 20 баллов в рейтинг студента)
«4», если	39 - 44 правильный ответ (добавляется 13 - 16 баллов в рейтинг студента)
«3», если	33 - 38 правильных ответов (добавляется 10 - 12 баллов в рейтинг студента)

Итоговый рейтинг студента формируется следующим образом:

№ п/п	Вид учебной деятельности	баллы	Максимально за 1 семестр
1.	Ведение конспекта лекций (за лекцию)	0.5	9
2	Выполнение семинарских заданий (см. перечень заданий в прил. 1)	2	28
3	Премиальные баллы за интерес к изучению курса (за семестр):	10	10
	Зачет в сессию	8	8

Разработчик:

_____ доцент Глухов Н. И.

Программа составлена в соответствии с требованиями ФГОС ВО и учитывает рекомендации ПООП по направлению и профилю подготовки **10.03.01 Информационная безопасность**

Программа рассмотрена на заседании кафедры радиофизики и радиоэлектроники «01» марта 2022 г. Протокол № 6

И.о.зав. кафедрой Колесник С.Н.