Приложение 3

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

«ИРКУТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ФГБОУ ВО «ИГУ»

Кафедра радиофизики и радиоэлектроники

УТВЕРЖДАЮ

Декан _____ Буднев Н.М.

«31» августа 2021 г.

Наименование дисциплины (модуля) Б1. О.27 Основы информационной безопасности

Направление подготовки 10.03.01 Информационная безопасность

Направленность (профиль) подготовки Безопасность автоматизированных систем

Квалификация выпускника бакалавр

Форма обучения очная

Согласовано с УМК физического факультета

Протокол №308 от «31»августа 2021 г.

Председатель _____ Буднев Н.М.

Рекомендовано кафедрой радиофизики и радиоэлектроники:

Протокол № 1 от «30» августа 2021 г.

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

2021 г.

Содержание

I. Цели и задачи дисциплины (модуля):

Цели: раскрытие сущности и значения информационной безопасности и защиты информации, их места в системе национальной безопасности, определение теоретических, концептуальных, методологических и организационных основ обеспечения безопасности информации, классификация и характеристика составляющих информационной безопасности и защиты информации в системе экономической безопасности организации

Задачи:

1. изучение основных положений государственной политики в области обеспечения информационной безопасности Российской Федерации, основных понятий и методологических принципов создания систем защиты информации в системе экономической безопасности организации;
2. изучение видов защищаемой информации, угроз информационной безопасности, методов и средств обеспечения информационной безопасности, механизмов защиты информации, моделей безопасности, критериев оценки защищенности и обеспечения безопасности информационных систем.

II. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Учебная дисциплина (модуль) Б1.О.27 Основы информационной безопасности относится к обязательной части программы.

Перечень последующих учебных дисциплин, для которых необходимы знания, умения и навыки, формируемые данной учебной дисциплиной: Б1.О.33 Документоведение. Нормативные документы в сфере информационной безопасности, Б1.О.18 Защита и обработка конфиденциальных документов.

III. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Процесс освоения дисциплины направлен на формирование компетенции ОПК-1 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
ОПК-1. Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства;	ИДК$_{ОПК1.1}$ Адекватно оценивает значимость информации в современном обществе.	Знать: Знать: нормативно правовые и методические документы по защите информации, классификацию и характеристики составляющих информационной безопасности; Уметь: понимать значение информации в развитии современного общества, определять требования по обеспечению информационной безопасности; Владеть: навыками применения информационных технологий для поиска и обработки информации с целю обеспечения защиты информации.
	ИДК$_{ОПК1.2}$ Понимает роль информационных технологий и информационной безопасности в современном обществе.	Знать: классификацию и характеристики составляющих информационной безопасности и защиты информации в создаваемых и функционирующих информационных системах;

		Уметь: разрабатывать модели угроз и нарушителей информационной безопасности в системах безопасности хозяйствующих субъектов Владеть: принципами и правилами построения организационных структур системы управления с учетом поддержания выполнения комплекса мер по информационной безопасности хозяйствующих субъектов
	ИДК$_{ОПК1.3}$ Осознает потребности личности, общества и государства в реализации мер информационной безопасности.	Знать: виды защищаемой информации, угрозы информационной безопасности, методы и средства обеспечения информационной безопасности в создаваемых и функционирующих информационных системах; Уметь: определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности информационных систем хозяйствующих субъектов Владеть: административно-управленческими методами реализации комплекса мер по обеспечению информационной безопасности.

IV. СОДЕРЖАНИЕ И СТРУКТУРА ДИСЦИПЛИНЫ

Объем дисциплины составляет 4 зачетных единиц, 144 часов,

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 (в том числе, внеаудиторная СР, КСР)	
					Лекция	Семинар/ Практическое, лабораторное занятие/	Консультация		
1	2	3	4	5	6	7	8	9	10
1	**Раздел 1. Теория информационной безопасности**	2							
1.1	Введение	2			2			2	
1.2	Сущность и понятие информационной безопасности	2			2		0,5	2	
1.3	Значение информационной безопасности и ее место в системе национальной безопасности	2				2		2	Защита ЛР

1.4.	Современная Доктрина информационной безопасности Российской Федерации	2			4			2	
1.5	Современная Доктрина информационной безопасности Российской Федерации	2				2		2	Защита ЛР
2	**Раздел 2. Методология защиты информации**	2							
2.1.	Сущность и понятие защиты информации	2			6		0,5	2	
2.2	Цели и значение защиты информации	2				1		2	Защита ЛР
2.3	Теоретические и концептуальные основы защиты информации	2			6			2	
2.4	Теоретические и концептуальные основы защиты информации	2				1		2	Защита ЛР
2.5	Организационные основы и методологические принципы защиты информации	2			6			2	
2.6	Современные факторы, влияющие на защиту информации	2				1		2	Защита ЛР
2.7	Классификация конфиденциальной информации по видам тайны и степеням конфиденциальности	2			6			2	
2.8	Критерии, условия и принципы отнесения информации к защищаемой	2				1		2	Защита ЛР
2.9	Каналы и методы несанкционированного доступа к конфиденциальной информации	2			4			2	
2.10	Состав и классификация носителей защищаемой информации	2				1		2	Защита ЛР
2.11	Классификация видов, методов и средств защиты информации	2			4			4	
2.12	Классификация конфиденциальной информации по видам тайны и степеням конфиденциальности	2				1		4	Защита ЛР
2.13	Классификация защищаемой информации по собственникам и владельцам	2				1		4	Защита ЛР
2.14	Понятие и структура угроз защищаемой информации	2				1		4	Защита ЛР
2.15	Источники, виды и способы дестабилизирующего воздействия на защищаемую информацию	2				1		4	Защита ЛР
2.16	Причины, обстоятельства и условия дестабилизирующего воздействия на защищаемую информацию	2				1		4	Защита ЛР
2.17	Каналы и методы несанкционированного доступа к конфиденциальной информации	2				1		4	Защита ЛР

2.18	Направления, виды и особенности деятельности разведывательных служб по несанкционированному доступу к конфиденциальной информации	2				1		3	Защита ЛР
2.19	Объекты защиты информации	2				1		4	Защита ЛР
2.20	Кадровое и ресурсное обеспечение защиты информации	2				1		4	Защита ЛР
2.21	Технологическое обеспечение защиты информации	2				1		4	Защита ЛР
2.22	Назначение и структура систем защиты информации	2				1			Защита ЛР
3.0	Зачет		8						Тестирование

. работы (в том числе КСР) обучающихся по дисциплине

Семестр	Название раздела, темы	Самостоятельная работа обучающихся			Оценочное средство	Учебно-методическое обеспечение самостоятельной работы
		Вид самостоятельной работы	Сроки выполнения	Трудоемкость (час.)		
1	Проработка лекционного материала по теме «Сущность и понятие информационной безопасности»	Работа с книгой и конспектом, подготовка отчета по лабораторной работе	1 неделя	3	Устный опрос	Из списка литературы, конспект
2	Подготовка к практическому занятию по теме «Современная Доктрина ИБ Российской Федерации»	Работа с книгой и конспектом, подготовка отчета по лабораторной работе	1 неделя	3	Устный опрос	Из списка литературы, конспект
3	Подготовка к практическому занятию по теме «Цели и значение защиты информации»	Работа с книгой и конспектом, подготовка отчета по лабораторной работе	2 неделя	3	Устный опрос	Из списка литературы, конспект
4	Подготовка к практическому занятию по теме «Теоретические и концептуальные основы защиты информации»	Работа с книгой и конспектом, подготовка отчета по лабораторной работе	2 неделя	3	Устный опрос	Из списка литературы, конспект

Семестр	Название раздела, темы	Самостоятельная работа обучающихся			Оценочное средство	Учебно-методическое обеспечение самостоятельной работы
		Вид самостоятельной работы	Сроки выполнения	Трудоемкость (час.)		
5	Подготовка к практическому занятию по теме «Современные факторы, влияющие на защиту информации»	Работа с книгой и конспектом, подготовка отчета по лабораторной работе	3 неделя	3	Устный опрос	Из списка литературы, конспект
6	Подготовка к практическому занятию по теме «Критерии, условия и принципы отнесения информации к защищаемой»	Работа с книгой и конспектом, подготовка отчета по лабораторной работе	3 неделя	4	Устный опрос	Из списка литературы, конспект
7	Подготовка к практическому занятию по теме «Состав и классификация носителей защищаемой информации»	Работа с книгой и конспектом, подготовка отчета по лабораторной работе	4 неделя	4	Устный опрос	Из списка литературы, конспект
8	Подготовка к практическому занятию по теме «Классификация конфиденциальной информации по видам тайны и степеням конфиденциальности»	Работа с книгой и конспектом, подготовка отчета по лабораторной работе	5 неделя	4	Устный опрос	Из списка литературы, конспект
9	Подготовка к практическому занятию по теме «Классификация защищаемой информации по собственникам и владельцам»	Работа с книгой и конспектом, подготовка отчета по лабораторной работе	6 неделя	4	Устный опрос	Из списка литературы, конспект
10	Подготовка к практическому занятию по теме «Понятие и структура угроз защищаемой информации»	Работа с книгой и конспектом, подготовка отчета по лабораторной работе	7 неделя	4	Устный опрос	Из списка литературы, конспект
11	Подготовка к практическому занятию по теме «Источники, виды и способы дестабилизирующего воздействия на защищаемую информацию»	Работа с книгой и конспектом, подготовка отчета по лабораторной работе	8 неделя	4	Устный опрос	Из списка литературы, конспект

Семестр	Название раздела, темы	Самостоятельная работа обучающихся			Оценочное средство	Учебно-методическое обеспечение самостоятельной работы
		Вид самостоятельной работы	Сроки выполнения	Трудоемкость (час.)		
12	Подготовка к практическому занятию по теме «Причины, обстоятельства и условия дестабилизирующего воздействия на защищаемую информацию»	Работа с книгой и конспектом, подготовка отчета по лабораторной работе	9 неделя	4	Устный опрос	Из списка литературы, конспект
13	Подготовка к практическому занятию по теме «Каналы и методы несанкционированного доступа к конфиденциальной информации»	Работа с книгой и конспектом, подготовка отчета по лабораторной работе	10 неделя	4	Устный опрос	Из списка литературы, конспект
14	Подготовка к практическому занятию по теме «Направления, виды и особенности деятельности разведывательных служб по несанкционированному доступу к конфиденциальной информации»	Работа с книгой и конспектом, подготовка отчета по лабораторной работе	11 неднля	4	Устный опрос	Из списка литературы, конспект
15	Подготовка к практическому занятию по теме «Объекты защиты информации»	Работа с книгой и конспектом, подготовка отчета по лабораторной работе	12 неделя	4	Устный опрос	Из списка литературы, конспект
16	Подготовка к практическому занятию по теме «Кадровое и ресурсное обеспечение защиты информации»	Работа с книгой и конспектом, подготовка отчета по лабораторной работе	13 неделя	4	Устный опрос	Из списка литературы, конспект
17	Подготовка к практическому занятию по теме «Технологическое обеспечение защиты информации»	Работа с книгой и конспектом, подготовка отчета по лабораторной работе	14 неделя	4	Устный опрос	Из списка литературы, конспект
18	Подготовка к практическому занятию по теме «Назначение и структура систем защиты информации»	Работа с книгой и конспектом, подготовка отчета по лабораторной работе	15-16 неделя	4	Устный опрос	Из списка литературы, конспект

Семестр	Название раздела, темы	Самостоятельная работа обучающихся			Оценочное средство	Учебно-методическое обеспечение самостоятельной работы
		Вид самостоятельной работы	Сроки выполнения	Трудоемкость (час.)		
19	Проработка теоретической части курсовой работы	Работа с книгой и конспектом, подготовка отчета по лабораторной работе	17-18 неделя	3	Устный опрос	Из списка лителатуры, конспект
20	Разработка практической части курсовой работы	Работа с книгой и конспектом, подготовка отчета по лабораторной работе	19-20 неделя	3	Устный опрос	Из списка лителатуры, конспект

4.3. Содержание учебного материала

Т 1. Введение.

Сущность и понятие информационной безопасности. Значение информационной безопасности и ее место в системе национальной безопасности. Современная Доктрина информационной безопасности Российской Федерации. Сущность и понятие защиты информации.

Т 2. Цели и значение защиты информации

Т4. Теоретические и концептуальные основы защиты информации

Т5. Организационные основы и методологические принципы защиты информации

Т6. Современные факторы, влияющие на защиту информации

Т7. Классификация конфиденциальной информации по видам тайны и степеням конфиденциальности

Т8. Критерии, условия и принципы отнесения информации к защищаемой

Т9. Понятие и структура угроз защищаемой информации

Т10. Источники, виды и способы дестабилизирующего воздействия на защищаемую информацию

Т11. Причины, обстоятельства и условия дестабилизирующего воздействия на защищаемую информацию

Т12. Каналы и методы несанкционированного доступа к конфиденциальной информации

Т13. Направления, виды и особенности деятельности разведывательных служб по несанкционированному доступу к конфиденциальной информации

Т14.Объекты защиты информации

4.3.1. 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	В.Т1.	Значение информационной безопасности и ее место в системе национальной безопасности	2		Письменный текущий контроль. Защита ЛР	ИДК$_{ОПК1.}$
2	Т2.	Современная Доктрина информационной безопасности Российской Федерации	2		Письменный текущий контроль. Защита ЛР	ИДК$_{ОПК1.2}$
3	Т3.	Цели и значение защиты информации	1		Письменный текущий контроль. Защита ЛР	ИДК$_{ОПК1.}$
4…	Т4.	Теоретические и концептуальные основы защиты информации	1		Письменный текущий контроль. Защита ЛР	ИДК$_{ОПК1.3}$

	Т5.	Современные факторы, влияющие на защиту информации	1		Письменный текущий контроль. Защита ЛР	ИДК$_{ОПК1.}$ ИДКОПК1.3
	Т6.	Критерии, условия и принципы отнесения информации к защищаемой	1		Письменный текущий контроль. Защита ЛР	ИДК$_{ОПК1.3}$
	Т7.	Состав и классификация носителей защищаемой информации	1		Письменный текущий контроль. Защита ЛР	ИДК$_{ОПК1.3}$
	Т8.	Классификация конфиденциальной информации по видам тайны и степеням конфиденциальности	1		Письменный текущий контроль. Защита ЛР	ИДК$_{ОПК1.2}$ ИДКОПК1.3
	Т9.	Понятие и структура угроз защищаемой информации	1		Письменный текущий контроль. Защита ЛР	ИДК$_{ОПК1.3}$
	Т10.	Источники, виды и способы дестабилизирующего воздействия на защищаемую информацию	1		Письменный текущий контроль. Защита ЛР	ИДК$_{ОПК1.2}$
	Т11.	Причины, обстоятельства и условия дестабилизирующего воздействия на защищаемую информацию	1		Письменный текущий контроль. Защита ЛР	ИДК$_{ОПК1.3}$
	Т12.	Каналы и методы несанкционированного доступа к конфиденциальной информации	1		Письменный текущий контроль. Защита ЛР	ИДК$_{ОПК1.2}$
	Т13.	Направления, виды и особенности деятельности разведывательных служб по несанкционированному доступу к конфиденциальной информации	4		Письменный текущий контроль. Защита ЛР	ИДК$_{ОПК1.}$ ИДКОПК1.2 ИДКОПК1.3
	Т14.	Объекты защиты информации	2		Письменный текущий контроль.	ИДК$_{ОПК1.2}$ ИДКОПК1.3

					Защита ЛР	

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	Введение. Т1. Значение информационной безопасности и ее место в системе национальной безопасности. Современная Доктрина информационной безопасности Российской Федерации	Осмысление материала лекций. Подготовка к Л.Р.1.	ОПК-1	ИДК $_{ОПК1.1}$ ИДК $_{ОПК1.2}$ ИДК $_{ОПК1.3}$
2.	Т2. Современная Доктрина информационной безопасности Российской Федерации.	Осмысление материала лекций. Подготовка к Л.Р.2.	ОПК-1	ИДК $_{ОПК1.1}$ ИДК$_{ОПК1.2}$ ИДК $_{ОПК1.3}$
3.	Т3. Цели и значение защиты информации	Осмысление материала лекций. Подготовка к Л.Р.3.	ОПК-1	ИДК $_{ОПК1.1}$ ИДК $_{ОПК1.2}$ ИДК $_{ОПК1.3}$
4.	Т4. Теоретические и концептуальные основы защиты информации	Осмысление материала лекций. Подготовка к Л.Р.4.	ОПК-1	ИДК $_{ОПК1.1}$ ИДК $_{ОПК1.2}$
5.	Т5. Организационные основы и методологические принципы защиты информации	Осмысление материала лекций. Подготовка к Л.Р.5.	ОПК-1	ИДК $_{ОПК1.1}$ ИДК $_{ОПК1.2}$
6.	Т.6 Классификация конфиденциальной информации по видам тайны и степеням конфиденциальности	Осмысление материала лекций. Подготовка к Л.Р.1.	ОПК-1	ИДК $_{ОПК1.1}$ ИДК $_{ОПК1.2}$
7.	Т7. Каналы и методы несанкционированного доступа к конфиденциальной информации	Осмысление материала лекций. Подготовка к Л.Р.6.	ОПК-1	ИДК $_{ОПК1.1}$
8.	Т8.Классификация видов, методов и средств защиты информации	Осмысление материала лекций.	ОПК-1	ИДК $_{ОПК1.2}$ ИДК $_{ОПК1.3}$

		Подготовка к Л.Р.7.		

4.4. Методические указания по организации самостоятельной работы студентов

Самостоятельная работа бакалавров – индивидуальная учебная деятельность, осуществляемая без непосредственного руководства преподавателя, в ходе которой бакалавр активно воспринимает, осмысливает полученную информацию, решает теоретические и практические задачи.

На самостоятельную работу выносятся следующие вопросы и задания по темам дисциплины:

Введение.

Т1. Значение информационной безопасности и ее место в системе национальной безопасности. Современная Доктрина информационной безопасности Российской Федерации.

Т2. Современная Доктрина информационной безопасности Российской Федерации.

Т3. Цели и значение защиты информации

Т4. Теоретические и концептуальные основы защиты информации

Т5. Организационные основы и методологические принципы защиты информации

Т.6 Классификация конфиденциальной информации по видам тайны и степеням конфиденциальности

Т7. Каналы и методы несанкционированного доступа к конфиденциальной информации

Т8. Классификация видов, методов и средств защиты информации.

Контроль самостоятельной работы проводится на практических занятиях, при защите лабораторных работ.

4.4. Примерная тематика курсовых работ (проектов) не предусмотрено

V. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Электронная информационно-образовательная среда университета обеспечивает доступ к электронным учебным изданиям и электронным образовательным ресурсам, указанным в рабочей программе дисциплины (модуля).

Библиотечный фонд укомплектован печатными зданиями из расчета не менее 0,25 экземпляра каждого из изданий на одного обучающегося из числа лиц, одновременно осваивающих соответствующую дисциплину (модуль).

1. Ю.Н. Загинайлов Теория информационной безопасности и методология защиты информации: учебное пособие [Электронный ресурс] //biblioclub.ru/index.php? page=book&id=276557 М.; Берлин: Директ-Медиа, 2015 100% онлайн.

2. С.А. Нестеров Основы информационной безопасности: Учебное пособие [Электронный ресурс] //biblioclub.ru/index.php? page=book&id=363040 СПб.: Политехнический университет, 2014 100% онлайн.

б) периодические издания

в) список авторских методических разработок:

г) базы данных, информационно-справочные и поисковые системы

1. Научная библиотека ИГУ *http://library.isu.ru/ru/resources/edu_resources/index.html*

2. БД книг и продолжающихся изданий http://ellibnb.library.isu.ru/cgi-bin/irbis64r_15/cgiirbis_64.htm?LNG=&C21COM=F&I21DBN=IRCAT&P21DBN=IRCAT

3. Электронный читальный зал «БиблиоТех» https://isu.bibliotech.ru/.

4. Электронная библиотечная система «Издательство «Лань» http://e.lanbook.com.
5. Электронная библиотечная система «РУКОНТ» http://rucont.ru.

VI.МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Учебно-лабораторное оборудование:

Класс ЭВМ, аудитория 323А, оснащенная вычислительной техникой, специальным ПО и свободным доступом в сеть Internet.

6.2. Программное обеспечение:

1. ABBY PDF Transformer 3.0 Пакет из 10 неименных лицензий Per Seat (10лиц.) EDU. Код позиции: AT30-1S1P10-102 Котировка № 03-165-11 от 23.11.2011. Бессрочно.
2. Microsoft OfficeProPlus 2013 RUS OLP NL Acdmc. Контракт № 03-013-14 от 08.10.2014.Номер Лицензии Microsoft 45936786. Бессрочно.
3. WinPro10 Rus Upgrd OLP NL Acdmc. Сублицензионный договор № 502 от 03.03.2017 Счет № ФРЗ- 0003367 от 03.03.2017 Акт № 4496 от 03.03.2017 Лицензия № 68203568. Бессрочно.
4. Kaspersky Free (ежегодно обновляемое ПО). Условия использования по ссылке: http://www.kaspersky.ru/free-antivirus/ . Бессрочно.

6.3. Технические и электронные средства:

Мультимедийный проектор, экран (по необходимости), меловая или маркерная доска.

VII.ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

На лекциях используются активные методы обучения (компьютерных симуляций, разбор конкретных ситуаций). Практические занятия проводятся в интерактивной форме. Лабораторные работы проводятся с использованием ПЭВМ с последующей защитой.

VIII.ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Текущий контроль реализуется в виде письменного текущего контроля на ПЗ1-ПЗ6, при защите лабораторных работ ЛР1-ЛР3. Текущий контроль направлен на выявление сформированности компетенции ПК-1.

Для реализации текущего контроля используется балльно-рейтинговая система оценки, принятая в университете.

За посещение одного вида занятия дается 0,6 балла (25 занятий (Л+Пз+ЛР)*0,6 балла = 15 баллов), максимальное количество баллов за письменный контроль на СКР – 5 баллов, за Пз – 54 баллов (6 летучек *5 балла= 30 баллов, решение задач у доски или самостоятельное досрочное решение всех задач, выносимых на ПЗ – 6 занятий*4 балла=24 баллов), лабораторные работы (ЛР) – 30 баллов (3*ЛР*10 баллов=30 баллов).

Параметры оценочного средства для письменного текущего контроля и решения задачи у доски или самостоятельного досрочного решения всех задач, выносимых на ПЗ1-ПЗ6. Параметры оценочного средства для КСР.

Критерии оценки	Оценка / баллы			
	Отлично 5 баллов.	Хорошо 3,5 балла	Удовлетв. 2 балла.	Неудовл. 0 баллов
Выполнение заданий	Полностью и корректно выполнены все задания.	Полностью выполнены все задания, допущены одна – две ошибки.	Не полностью выполнены задания, допущены одна – две ошибки.	Задание не выполнены или задание выполнено не полностью и

		.		допущено более 3-х ошибок. .

Параметры оценочного средства для защиты лабораторных работ ЛР1-ЛР3

Критерии оценки	Оценка / баллы			
	Отлично 7-10 баллов	Хорошо 4-6 балла	Удовлетв. 1-3 балла.	Неудовл. 0 баллов
Выполнение заданий	Полностью и корректно оформлен отчет, сделаны выводы. При защите показано всестороннее и глубокое знание материала.	В целом отчет оформлен корректно, сделаны выводы, но имеются незначительные недостатки. При защите студент показывает понимает материала, приводит примеры, но испытывает затруднения с выводами, однако достаточно полно отвечает на дополнительные вопросы.	Отчет оформлен полностью. Имеются замечания по оформлению, выводы сделаны не полностью. При защите - суждения поверхностны, содержат ошибки, примеры не приводятся, ответы на дополнительные вопросы не уверенные.	Отчет не оформлен. Отчет оформлен со значительными замечаниями, выводы не полные, при защите студент с трудом формулирует свои мысли, не приводит примеры, не дает ответа на дополнительные вопросы .

Вопросы для письменного текущего контроля приведены ниже:

1. Структура государственной системы защиты информации (схема).
2. Система документации по технической защите информации (схема).
3. Действующие документы по защите информации с учетом категорий доступа к ней и видов информационных систем.
4. Определение информационной безопасности.
5. Определение защиты информации.
6. Меры по обеспечению информационной безопасности.
7. Основные организационно-технические мероприятиям по защите информации.
8. Источники угрозы информационной безопасности.
9. Угрозы информационной безопасности.
10. Уязвимости информационной безопасности.
11. Атаки информационной безопасности.
12. Построить логическую цепочку реализации угрозы информационной безопасности.
13. Построить схему классификации источников угроз ИБ.
14. Объективные уязвимости.
15. Субъективные уязвимости.

16. Случайные уязвимости.
17. Понятие лицензии (пользовательская лицензия).
18. Определение лицензионной политики.
19. Понятие коммерческой лицензии.
20. Понятие открытой лицензии.
21. Гарантируемые права открытой лицензии.
22. Понятие нелицензионного программного обеспечения.
23. Угрозы при использовании нелицензионного программного обеспечения.
24. Закон, определяющий правовые основы информационной безопасности (наименование, когда принят, основные требования).

Перечень примерных вопросов для защиты лабораторных работ:

ЛР1.Значение информационной безопасности и ее место в системе национальной безопасности.

ЛР2.Современная Доктрина информационной безопасности Российской Федерации.

ЛР3.Цели и значение защиты информации. Теоретические и концептуальные основы защиты информации.

ЛР4.Организационные основы и методологические принципы защиты информации.

ЛР5.Классификация конфиденциальной информации по видам тайны и степеням конфиденциальности.

ЛР6. Каналы и методы несанкционированного доступа к конфиденциальной информации.

ЛР7. Классификация видов, методов и средств защиты информации.

Оценочные средства для промежуточной аттестации (в форме зачета).

Форма промежуточного контроля – зачет. Зачет выставляется по итогам изучения дисциплины в течение семестра при условии положительных результатов защиты всех лабораторных работ, предусмотренных программой.

Промежуточная аттестация направлена на проверку сформированности компетенций ОПК-1 и проводится в форме тестирования. Для реализации промежуточного контроля используется балльно-рейтинговая система оценки, принятая в университете.

Зачет выставляется по сумме балов, полученных при изучении дисциплины.

Усвоение бакалавром изучаемой дисциплины максимально оценивается 100 баллами. Из них 90 баллов обучающийся может набрать в течение семестра и от 0 до 10 баллов могут быть даны в качестве «премиальных» баллов за активные формы работы, высокое качество выполненных лабораторных и т.д.

Параметры оценочного средства для аттестации в форме зачета.

Итоговый семестровый рейтинг	Академическая оценка
0-59 баллов	«не зачтено»
60-100 баллов	«зачтено»

Материалы для проведения текущего и промежуточного контроля знаний студентов:

Пример теста для проведения промежуточной аттестации в форме зачета

Вариант 1

1. Определение термина «информация»:

А - совокупность содержащихся в базах данных сведений;

Б - сведения (сообщения, данные) независимо от формы их представления.
В - сведения (сообщения, данные) воспроизводимые различными системами.
2. Определение термина «обладатель информации»:
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.
3. Технические способы защиты информации в зависимости от используемых средств классифицируются как:
А - полуактивные;
Б - пассивные;
В – разноплановые.
4. Указать меры, которые устанавливаются для обеспечения правового режима защиты персональных данных;
5. Указать источники права в области оборота сведений составляющих коммерческую тайну;
6. Если сведения относятся к государственной тайне проанализировать порядок установления степени их секретности.
7. Пассивные способы защиты информации:
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.
8. Несанкционированный доступ к информации»:
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.
9. Предоставление информации -
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.
10. Построить схему реализации угрозы информационной безопасности в атаку.
11. Защита информации представляет собой принятие мер, перечислить.
12. Исходя из требований № 149-ФЗ защиту информации можно разделить так же на несколько уровней:
13. Свойства безопасности информации, перечислить.
14. Способы и методы защиты электронного документооборота, назвать.
15. Риск информационной безопасности:
А – потенциальная возможность использования уязвимостей активов конкретной угрозой для причинения ущерба организации.
Б – потенциальная возможность нанесения ущерба в результате действия угроз информационной безопасности;
В – возможность реализации угрозы информационной безопасности;

Г – неудовлетворительное состояние системы защиты информации.

Вариант 2

1. Перечень объектов информатизации, на которые распространяется требования по аттестации:

А. Значимых объектов критической информационной инфраструктуры Российской Федерации;

Б. Информационных систем персональных данных (за исключением государственных, муниципальных информационных систем персональных данных);

С. Автоматизированных систем управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды.

Д. Помещений, предназначенных для ведения конфиденциальных переговоров (далее - защищаемые помещения)

2. Аттестация объектов информатизации –определение.

А. Комплекс организационно-технических мероприятий, результатом которого является документ «Аттестат соответствия», подтверждающий выполнение на объекте информатизации норм и правил, определенных действующим законодательством Российской Федерации.

Б. Проведение комплекса организационных и технических мероприятий и работ по защите информации.

С. Проверка уровня защиты информации на объекте информатизации.

Д. Оценка уровня защиты информации включая эффективность технических и программно-технических средств защиты.

2. Условия обязательной аттестация объектов информатизации.

А. Государственных и муниципальных информационных систем, в том числе государственных, муниципальных информационных систем персональных данных.

Б. Информационных систем управления производством, используемых организациями оборонно-промышленного комплекса, в том числе автоматизированных систем станков с числовым программным управлением.

С. Значимых объектов критической информационной инфраструктуры Российской Федерации.

Д. Помещений, предназначенных для ведения конфиденциальных переговоров.

4. Цели проведения аттестации объекта информатизации

А. Оценка уровня защиты объекта информатизации.

Б. Оценка соответствия внедренного комплекса мер по защите информации и установленных на объекте информатизации средств защиты информации требуемому уровню защищенности информации.

С. Получения лицензии организации для осуществления деятельности по защите информации.

Д. Оценка текущего состояния средств защиты информации по противодействию угроз.

5. В ходе аттестационных испытаний объекта информатизации владельцем объекта информатизации могут вноситься изменения в объект информатизации.

А. Да.

Б. Нет.

С. Да, только в случае наличия необходимой документации на объекте.

Д. По согласованию с федеральным органом исполнительной власти в области защиты информации.

6. Состав разделов программы и методики аттестационных испытаний.

А. Общие положения;

Б. Перечень необходимых документов

С. Программа аттестационных испытаний объекта информатизации

Д. Методики аттестационных испытаний объекта информатизации

7. Перечень мероприятий аттестационных испытаний.

А. Обследование объекта информатизации на предмет оценки соответствия объекта информатизации и условий его эксплуатации требованиям по защите информации, а также документам, предусмотренным пунктом 11 настоящего Порядка;

Б. Проверку наличия у владельца объекта информатизации работников, ответственных за обеспечение защиты информации в ходе эксплуатации объекта информатизации

С. Оценку соответствия принятых на объекте информатизации организационных мер требованиям по защите информации и их достаточности для защиты от актуальных для объекта информатизации угроз безопасности информации;

Д. Оценку эффективности защиты (защищенности) информации от утечки по техническим каналам (только для защищаемых помещений).

8. Аттестация объекта информатизации проводится:

А. На этапе смены собственника объекта информатизации.

Б. На этапе эксплуатации.

С. На этапе создания или развития (модернизации)

Д. На этапе создания.

9. Аттестат соответствия выдается на срок:

А. 5 лет.

Б. 3 года.

С. На весь эксплуатации объекта информатизации.

Д. 2 года.

10. Условия приостановки действия аттестата соответствия.
А. Установления факта несоответствия аттестованного объекта информатизации требованиям по защите информации, в результате чего имеется или имелась возможность возникновения угроз безопасности информации.

Б. Не устранения недостатков, выявленных ФСТЭК России (территориальным органом ФСТЭК России) в соответствии с пунктом 30 настоящего Порядка.

С. Непредставления протоколов контроля уровня защиты информации на аттестованном объекте информатизации.

Д. Обращения владельца объекта информатизации о приостановлении действия аттестата соответствия.

11. Условия прекращения действия аттестата соответствия.
А. Непредставления владельцем объекта информатизации в установленный в уведомлении о приостановлении действия аттестата соответствия срок материалов, подтверждающих устранение недостатков.

Б. Непредставления владельцем объекта информатизации в установленный в уведомлении о приостановлении действия аттестата соответствия срок протоколов контроля уровня защищенности информации на аттестованном объекте информатизации;

С. Непредставления владельцем объекта информатизации в установленный в уведомлении о приостановлении действия аттестата соответствия срок материалов, подтверждающих проведение аттестации объекта информатизации для измененной архитектуры системы защиты информации;

Д. Обращения владельца объекта информатизации о прекращении действия аттестата соответствия.

12. Действие аттестата соответствия может быть приостановлено на срок:
А. Не более 30 календарных дней.

Б. Не более 10 календарных дней.

С. Не более 90 календарных дней.

Д. Не более 3х календарных дней.

13. Функции ФСТЭК при аттестации объекта информатизации.
А. Орган по аттестации объектов информатизации.

Б. Федеральный орган исполнительной власти

С. Орган местного самоуправления.

Д. Надзорный орган.

14. Решение о прекращении действия аттестата соответствия оформляется:
А. Приказом руководителя субъекта информатизации.

Б. Приказом ФСТЭК России (территориального органа ФСТЭК России).

С. Решением суда.

Д. Приказом вышестоящей организации субъекта информатизации.

№	Вид контроля	Контролируемые темы (разделы)	Контролируемые компетенции/ индикаторы
1	**2**	**3**	**4**
1	Тестовое задание	Т1-Т14	ОПК-1. ИДК $_{ОПК1.1}$ ИДК $_{ОПК1.2}$

Разработчики:

Доцент кафедры РФиРЭ _____ Серёдкин С.П.

Программа рассмотрена на заседании кафедры радиофизики и радиоэлектроники «30» августк 2021 г. протокол № 1

И.О. зав. кафедрой Колесник С.Н.