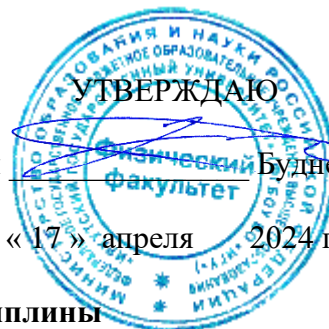




**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ**

федеральное государственное бюджетное образовательное учреждение
высшего образования
«ИРКУТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ФГБОУ ВО «ИГУ»

Кафедра радиофизики и радиоэлектроники



Декан  Буднев Н.М.

«17» апреля 2024 г.

Рабочая программа дисциплины

Наименование дисциплины **Б1.О.20 Основы управления информационной безопасностью**

Направление подготовки **10.03.01 Информационная безопасность**

Направленность (профиль) подготовки **Техническая защита информации**

Квалификация выпускника **бакалавр**

Форма обучения **очная**

Согласовано с УМК физического факультета

Протокол №42 от «15» апреля 2024 г.

Председатель  Буднев Н.М.

Рекомендовано кафедрой радиофизики и радиоэлектроники:

Протокол № 8 от «8» апреля 2024 г.

И.О. зав. кафедрой  Колесник С.Н.

Иркутск 2024 г.

Содержание

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ.....	3
2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО.....	3
3. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ.....	3
4. СОДЕРЖАНИЕ И СТРУКТУРА ДИСЦИПЛИНЫ.....	5
4.1. Содержание дисциплины, структурированное по темам, с указанием видов учебных занятий и отведенного на них количества академических часов.....	5
4.2. План внеаудиторной самостоятельной работы обучающихся по дисциплине.....	6
4.3. Содержание учебного материала	8
4.3.1. Перечень семинарских, практических занятий и лабораторных работ.....	9
4.3.2. Перечень тем (вопросов), выносимых на самостоятельное изучение студентами в рамках самостоятельной работы (СРС).....	10
4.4. Методические указания по организации самостоятельной работы студентов.....	12
4.5. Примерная тематика курсовых работ.....	12
5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ	13
а) основная литература.....	13
б) дополнительная литература.....	13
в) базы данных, информационно-справочные и поисковые системы.....	13
6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ.....	13
6.1. Учебно-лабораторное оборудование.....	13
6.2. Программное обеспечение.....	13
6.3. Технические и электронные средства.....	13
7. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ.....	13
8. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ.....	14

I. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

Цели и задачи дисциплины «Основы управления информационной безопасностью»

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) «**Техническая защита информации**», а также изучение теоретических, методологических и практических проблем формирования, функционирования и развития систем управления информационной безопасностью и защитой информации

Задачи:

- направленность на многоуровневую систему образования и непрерывность профессионального развития;
- обеспечение обучающимися выбора индивидуальной образовательной траектории;
- 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 «**Основы управления информационной безопасностью**» 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: «Комплексная система защиты информации», «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
ОПК-8; Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности;	ИДКОПК8.1. Подбирает и изучает научно-техническую литературу, нормативную и методическую документацию для решения задач профессиональной деятельности.	<p>Знать: научно-техническую литературу, нормативную и методическую документацию для решения задач профессиональной деятельности.</p> <p>Уметь: осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности;</p> <p>Владеть: навыками по подбору, изучению и обобщению научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности;</p>
	ИДКОПК8.2. Обобщает и анализирует информацию из научно-технической литературы, нормативной и методической документации для решения задач профессиональной деятельности.	<p>Знать: методику по обобщению и анализу научно-технической литературы, нормативной и методической документации для решения задач профессиональной деятельности.</p> <p>Уметь: осуществлять подбор, по обобщению и анализу научно-технической литературы, нормативной и методической документации для решения задач профессиональной деятельности;</p>

		Владеть: навыками по подбору, изучению, обобщению и анализу научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности
--	--	---

IV. СОДЕРЖАНИЕ И СТРУКТУРА ДИСЦИПЛИНЫ

Объем дисциплины составляет 4 зачетных единиц, 144 часа,
в том числе зачетных единиц, 17 часов на экзамен

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

Форма промежуточной аттестации: экзамен

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

№ п/п	Раздел дисциплины/тема	Семестр	Всего часов	Из них практическая подготовка обучающихся	Виды учебной работы, включая самостоятельную работу обучающихся, практическую подготовку и трудоемкость (в часах)			Самостоятельная работа	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	Раздел 1. Система управления информационной безопасностью	8								
2	Системный подход к проектированию, внедрению и поддержанию системы обеспечения ИБ на предприятии информационных ресурсов и защиты	8			6					

	информации /Лек/								
3	Проработка лекционного материала «Системный подход к проектированию, внедрению и поддержанию системы обеспечения ИБ на предприятии» /Ср/	8						7	
4	Политика безопасности /Пр/	8				6			
5	Проработка материала «Политика безопасности» /Ср/	8						7	
6	Аудит информационной безопасности /Лек/	8			6				
7	Подготовка к семинарским занятиям; «Аудит информационной безопасности» /Ср/	8						7	
8	Организация обеспечения информационной безопасности автоматизированных систем /Пр/	8				8			
9	Проработка материала «Организация обеспечения информационной безопасности автоматизированных систем» /Ср/	8						7	
10	Раздел 2. Управление комплексной системой защиты информации								
11	Назначение, структура и содержание управления комплексной системой защиты информации /Лек/	8			4				
12	Проработка лекционного материала Назначение, структура и содержание управления комплексной системой защиты информации /Ср/	8						7	
13	Принципы и методы планирования комплексной системы защиты информации /Пр/	8				6			
14	Проработка лекционного материала «Принципы и методы планирования функционирования комплексной системы защиты информации» /Ср/	8						7	
15	Сущность и содержание контроля функционирования комплексной системы защиты информации /Лек/	8			4				
16	Проработка лекционного материала «Сущность и содержание контроля функционирования комплексной системы защиты информации» /Ср/	8						7	
17	Общая характеристика подходов к оценке эффективности систем защиты информации /Пр/	8				6			
18	Проработка лекционного материала «Общая характеристика подходов к оценке эффективности систем защиты информации» /Ср/	8						7	
19	Методы и модели оценки эффективности комплексной системы защиты информации /Лек/	8			6				
20	Методы и модели оценки эффективности комплексной системы защиты информации /Ср/	8						8	

21	Раздел 3. Контроль знаний							
22	Подготовка к промежуточной аттестации (Экзамен)	8			26	26		64
								17 (Экзамен)

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	Проработка лекционного материала «Системный подход к проектированию, внедрению и поддержанию системы обеспечения ИБ на предприятии» /Ср/	внеаудиторная	1-2 неделя	5	Выполнение заданий по семинарским работам	Источники 1,2 из основной литературы и 1 из дополнительной
8	Проработка материала «Политика безопасности» /Ср/	внеаудиторная	2-3 неделя	5	Выполнение заданий по семинарским работам	Источники 1,2 из основной литературы и 1 из дополнительной
8	Подготовка к семинарским занятиям; «Аудит информационной безопасности» /Ср/	внеаудиторная	3-4 неделя	5	Выполнение заданий по семинарским работам	Источники 1,3 из основной литературы и 2 из дополнительной
8	Проработка материала «Организация обеспечения информационной безопасности автоматизированных систем» /Ср/	внеаудиторная	4-5 неделя	5	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	Проработка лекционного материала «Сущность и задачи комплексной системы защиты информации. Понятие и сущность КСЗИ. Назначение КСЗИ. Задачи КСЗИ» /Ср/	внеаудиторная	5-6 неделя	5	Выполнение заданий по семинарским работам	Источники 1,3 из основной литературы и 2 из дополнительной
8	Проработка лекционного материала Назначение, структура и содержание управления комплексной системой защиты информации /Ср/	внеаудиторная	7-8 неделя	5	Выполнение заданий по семинарским работам	Источники 1,5 из основной литературы и 3 из дополнительной
8	Проработка лекционного материала «Принципы и методы планирования функционирования комплексной системы защиты информации» /Ср/	внеаудиторная	8-9 неделя	5	Выполнение заданий по семинарским работам	Источники 1,6 из основной литературы и 3 из дополнительной
8	Проработка лекционного материала «Сущность и содержание контроля функционирования комплексной системы защиты информации» /Ср/	внеаудиторная	9-10 неделя	5	Выполнение заданий по семинарским работам	Источники 1,6 из основной литературы и 3 из дополнительной
8	Проработка лекционного материала «Общая характеристика подходов к оценке эффективности систем защиты информации» /Ср/	внеаудиторная	10-11 неделя	5	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	Проработка лекционного материала Назначение, структура и содержание управления комплексной системой защиты информации /Ср/	внеаудиторная	11-12 неделя	5	Выполнение заданий по семинарским работам	Источники 2,1 из основной литературы и 4 из дополнительной
8	Проработка лекционного материала «Общая характеристика подходов к оценке эффективности систем защиты информации» /Ср/	внеаудиторная	14-15 неделя	5		
8	Методы и модели оценки эффективности комплексной системы защиты информации /Ср/	внеаудиторная	14-15 неделя	5		
8	Подготовка к сдаче экзамена	внеаудиторная	15-16 неделя	4	Выполнение заданий по семинарским работам	Источники 1-1-2-2 из основной литературы и 1-4 из дополнительной
Общий объем самостоятельной работы по дисциплине (час)				64		
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

№ 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	Политика безопасности /Пр/	6		Выполнение заданий по вопросам семинара	ИДК _{ОПК8.1.}
2	1	Организация обеспечения информационной безопасности автоматизированных систем /Пр/	8		Выполнение заданий по вопросам семинара	ИДК _{ОПК8.1.}
3	2	Принципы и методы планирования комплексной системы защиты информации /Пр/	6		Выполнение заданий по вопросам семинара	ИДК _{ОПК8.2.}
4	2	Общая характеристика подходов к оценке эффективности систем защиты информации /Пр	6		Выполнение заданий по вопросам семинара	ИДК _{ОПК8.2.}

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	Проработка лекционного материала «Системный подход к проектированию, внедрению и поддержанию системы обеспечения ИБ на предприятии»	Подготовка по вопросам семинара	ОПК-8	ИДК _{ОПК8.1.}
2	Проработка материала «Политика безопасности»	Подготовка по вопросам семинара	ОПК-8	ИДК _{ОПК8.1.}
3	Подготовка к семинарским занятиям; «Аудит информационной	Подготовка по вопросам семинара	ОПК-8	ИДК _{ОПК8.1.}

	безопасности»			
4	Проработка материала «Организация обеспечения информационной безопасности автоматизированных систем»	Подготовка по вопросам семинара	ОПК-8	ИДКОПК8.2
5	Проработка лекционного материала «Сущность и задачи комплексной системы защиты информации. Понятие и сущность КСЗИ. Назначение КСЗИ. Задачи КСЗИ»	Подготовка по вопросам семинара	ОПК-8	ИДКОПК8.2
6	Проработка лекционного материала Назначение, структура и содержание управления комплексной системой защиты информации	Подготовка по вопросам семинара	ОПК-8	ИДКОПК8.2
7	Проработка лекционного материала «Принципы и методы планирования функционирования комплексной системы защиты информации»	Подготовка по вопросам семинара	ОПК-8	ИДКОПК8.2
8	Проработка лекционного материала «Общая характеристика подходов к оценке эффективности систем защиты информации»	Подготовка по вопросам семинара	ОПК-8	ИДКОПК8.2
9	Проработка лекционного материала Назначение, структура и содержание управления комплексной системой защиты информации	Подготовка по вопросам семинара	ОПК-8	ИДКОПК8.2
10	Методы и модели оценки эффективности комплексной системы защиты информации	Подготовка по вопросам семинара	ОПК-8	ИДКОПК8.2
	Подготовка к промежуточной аттестации	Подготовка к экзамену	ОПК-8	ИДКОПК8.1, ИДКОПК8.2

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	А.А. Внуков	Управление информационной безопасности: Учебник [Электронный ресурс] « Юрайт», неограниченный доступ //biblioclub.ru/index.php?page=book&id=438331	ИГУ, 2022	100% Онлайн
Л14	М.А. Лапина, А.Г. Ревин,	Информационное право : учебное пособие [Электронный ресурс]	М. : Юнити-Дана, 2015	100% Онлайн

	В.И. Лапин	//biblioclub.ru/index.php?page=book&id=118624		
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 случаях – 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 I	ОПК-8	Защита реферата
2	Раздел II	ОПК-8	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.

Тест

1. Выберите правильное определение термина «информация»:
 - а) совокупность содержащихся в базах данных сведений;
 - б) совокупность содержащихся в базах данных сведений, зафиксированных на машинных носителях;
 - в) сведения (сообщения, данные) воспроизводимые различными системами;
 - г) сведения (сообщения, данные) независимо от формы их представления.
2. Выберите правильное 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;
 - г) лицо, самостоятельно создавшее информацию либо получившее право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.
3. Выберите правильное определение термина «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;
 - г) действия, направленные на получение информации как определённым, так и неопределённым кругом лиц или передачу информации как определенному, так и неопределённым кругом лиц.
4. Выберите правильное определение термина «защищаемые помещения»:
 - 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;
5. Выберите правильное определение термина «контролируемая зона»:
 - 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.

6. 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;

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

а) строительные материалы, используемые для отделки помещений, в которых размещаются отдельные элементы АС;

б) детали интерьера, используемые для размещения АИС;

в) средства контроля эффективности применения средств защиты информации;

г) средства контроля эффективности прочности ограждений;

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

8. 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.

9. «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.

10. Техническими каналами утечки информации 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;

11. «Несанкционированный доступ 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.

12. «Персональный идентификатор» — это

- а) устройство для хранения зашифрованной информации пользователя;
- б) устройство для хранения информации, необходимой при идентификации и аутентификации пользователя;
- в) устройство для хранения журнала аудита.

13. Механизм контроля целостности СЗИ Secret Net предназначен для

- а) формирования цифровых отпечатков данных;
- б) контроля информационных потоков;
- в) слежения за неизменностью содержимого ресурсов компьютера.

14. Механизм замкнутой программной среды СЗИ Secret Net и Dallas Lock предназначен для

- а) ограничения использования программного обеспечения на компьютере;
- б) установки ограниченного количества программ;
- в) сбора сведений об используемых приложениях.

15. В СЗИ Secret Net пользователю с уровнем допуска "конфиденциально" разрешается выполнять чтение файлов с категориями

- а) «конфиденциально»;
- б) «секретно»;
- в) «строго конфиденциально»,
- г) «неконфиденциально».

16. Длина ключа шифрования алгоритма ГОСТ 28147-89 равна

- а) 56 бит;
- б) 256 бит;
- в) 1024 бит;
- г) 128 бит.

17. К какому типу криптосистем относится алгоритм AES?

- а) несимметричные;
- б) асимметричные;
- в) симметричные;
- г) полусимметричные.

18. 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;
- г) выставление постов охраны у помещений, в которых размещаются технические средства обработки информации.

19. Межсетевой экран служит для:

- а) разграничения доступа в помещения АИС;
- б) фильтрации трафика при передачи данных;
- в) защиты от утечек информации путем экранирования стен;
- г) контроля целостности программного обеспечения.

20. Максимально возможное количество категорий конфиденциальности в СЗИ Secret Net 7.x равно _____ (16).

21. В СЗИ Secret Net категорию конфиденциальности можно назначить для следующих ресурсов: каталоги и файлы на дисках с файловой системой _____ (NTFS).

22. Практическая стойкость алгоритма RSA основана на сложности решения задачи _____ (факторизации).

23. Практическая стойкость алгоритма Диффи-Хеллмана основана на сложности решения задачи нахождения дискретного _____ (логарифма).

24. Эффективным средством защиты от утечки информации из АИС показали себя _____ (DLP) – системы.

25. Хэш-функции предназначены, главным образом, для контроля _____ (целостности) данных.

26. Технология электронной подписи разработана с целью подтверждения _____ (авторства) и _____ (подлинности) сообщений.

27. Длина хэш-кода алгоритма MD5 составляет _____ (128) бит.

28. Как в СЗИ Secret Net происходит включение режима хранения пароля в идентификаторе?

(Основной тезис: происходит добавление в базу данных Secret Net сведений о включении для пользователя режима хранения пароля в идентификаторе. Одновременно с этой операцией выполняется запись пароля в идентификатор. После включения режима пароль пользователя при входе в систему не вводится с клавиатуры, а считывается из идентификатора).

29. Каким образом в СЗИ Secret Net происходит присвоение пользователю персонального идентификатора?

(Основной тезис: происходит добавление в базу данных Secret Net сведений о том, что пользователю принадлежит персональный идентификатор данного типа с уникальным серийным номером).

30. Каким образом в СЗИ Secret Net реализуется затирание файлов?

(Основной тезис: при действии механизма затирания в область диска, где физически было расположено содержимое удаленного файла, записывается последовательность случайных чисел).

31. Что происходит при выборе способа очистки журнала СЗИ Secret Net при его переполнении «Затирать события по мере необходимости»?

(Основной тезис: при переполнении журнала система защиты автоматически удаляет из журнала необходимое количество самых старых записей).

32. Каким образом в СЗИ Secret Net реализуется настройка дискреционного разграничения доступа к файлам и папкам?

(Основной тезис: настройка дискреционного разграничения доступа к файлам и папкам производится штатными средствами операционной системы).

33. Кратко описать назначение и функции Удостоверяющего Центра в системе PCI.

Назначение оценочных средств текущего контроля – выявить сформированность компетенций (ОПК-5). Ниже приведен перечень оценочных средств текущего контроля:

1. **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	Полностью и	Полностью выполнены	Не полностью

заданий	корректно выполнены все задания (9-10 баллов)	все задания, допущены одна – две ошибки (7 -8 баллов)	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 – 33 вопроса.

Параметры оценочного средства

Предел длительности контроля	45 мин
Последовательность выборки вопросов из разделов (по всему курсу дисциплины)	случайная
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	Премияльные баллы за интерес к изучению курса (за семестр):	10	10
	Экзамен 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 «8» апреля 2024 г. Протокол № 8

И.о.зав. кафедрой  Колесник С.Н.

Настоящая программа, не может быть воспроизведена ни в какой форме без предварительного письменного разрешения кафедры-разработчика программы.