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.

« 20 » апреля 2023 г.

Рабочая программа дисциплины

Наименование дисциплины **Б1.В.ДВ.02.01 Программная защита информации**

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 №38 от «18» апреля 2023 г.

Председатель _____ Буднев Н.М.

Рекомендовано кафедрой радиофизики и радиоэлектроники:

Протокол № 7 от «27» февраля 2023 г.

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

Иркутск 2023 г.

Содержание

Стр.

I. Цели и задачи дисциплины (модуля)

II. Место дисциплины (модуля) в структуре ОПОП.

III. Требования к результатам освоения дисциплины (модуля)

IV. Содержание и структура дисциплины (модуля)

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

4.2 План внеаудиторной самостоятельной работы обучающихся по дисциплине

4.3 Содержание учебного материала

4.3.1 Перечень семинарских, практических занятий и лабораторных работ

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

4.4. Методические указания по организации самостоятельной работы студентов

4.5. Примерная тематика курсовых работ (проектов

V. Учебно-методическое и информационное обеспечение дисциплины (модуля)

а) перечень литературы

б) периодические издания

в) список авторских методических разработок

г) базы данных, поисково-справочные и информационные системы

VI. Материально-техническое обеспечение дисциплины (модуля)

6.1. Учебно-лабораторное оборудование:

6.2. Программное обеспечение:

6.3. Технические и электронные средства обучения:

VII. Образовательные технологии

VIII. Оценочные материалы для текущего контроля и промежуточной аттестации

1. Цели и задачи дисциплины (модуля):

Цель: изучение состояния проблем комплексного обеспечения информационной безопасности, методов и средств защиты информации в автоматизированных системах
Задачи:

1. изучение и принцип функционирования основных автоматизированных систем;
2. изучение основных приложений, прикладных систем и задач автоматизированных систем;
3. способы и требования организации работ по обеспечению защиты информации в автоматизированных системах.

I. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Учебная дисциплина (модуль) Б1.В.ДВ.02.01 Программная защита информации относится к вариативной части программы.

Перечень последующих учебных дисциплин, для которых необходимы знания, умения и навыки, формируемые данной учебной дисциплиной: Компьютерная защита информации от несанкционированного доступа.

II. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Процесс освоения дисциплины направлен на формирование компетенций ПК-2 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 анализ уязвимостей системы защиты информации и автоматизированных систем.	ИДК$_{ПК2.1}$ Проводит анализ уязвимостей системы защиты информации.	Знать Основные понятия и определения в области информационной безопасности автоматизированных систем (АС) принципы и стандарты построения современных защищенных АС; основные тенденции и закономерности развития средств и методов защиты информации в АС; политики безопасности и меры защиты в АС. Уметь: Анализировать текущее состояние ИБ на объекте с целью разработки требований к защищенным АС; Определять основные угрозы ИБ для АС; определять организационные, организационно-технические и технические средства, методы и мероприятия по защите информации на АС; Планировать стандартные решения для защиты информации в АС и квалифицированно оценивать их качество. Владеть: Терминологией и системным подходом построения защищенных открытых информационных систем (ОИС);
ПК-3. Способен внедрять организационные меры по защите информации в автоматизированных системах.	ИДК$_{ПК3.1}$ Внедряет организационные меры по защите информации в автоматизированных системах.	

		Навыками анализа угроз ИБ и уязвимостей в АС; Организационными, организационно-техническими, техническими и компьютерными средствами и методами по защите информации на АС .
	ИДК$_{ПК2.2}$ Проводит анализ уязвимостей автоматизированных систем.	Знать: Особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; Методы тестирования АС на наличие уязвимостей. Уметь: Идентифицировать и оценивать угрозы безопасности вредоносного информационного воздействия на АС, её компоненты в том числе на программное обеспечение. Выявлять уязвимости и угрозы информационной безопасности для АС. Определять методы для защиты информационных и технических ресурсов от несанкционированного межсетевого доступа. Оценивать критичность информации функционирующей, а АС и определять методы её защиты. Владеть: Навыками работы по нейтрализации вредоносного информационного воздействия на АС, её компоненты в том числе на программное обеспечение. Практическими навыками выявления уязвимостей и угроз информационной безопасности для АС. Способностью определять методы и средства для защиты информационных и технических ресурсов от несанкционированного межсетевого доступа в АС.

III. СОДЕРЖАНИЕ И СТРУКТУРА ДИСЦИПЛИНЫ

Объем дисциплины составляет 3 зачетных единицы, 108 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. Управление деятельностью предприятия; классификация автоматизированных систем (АС). Этапы разработки.**	8							
1.1	Информационный контур управления. АС как объект управления. Эволюция АС. Требования к АС. /Лек/	8			2			2	Конспект

1.3	Состав и формирование требований, проектируемых автоматизированных ИС /Лр/	8				4		1	Защита ЛР
1.5	АС оперативного управления. АС информационное, математическое и программное обеспечение. /Лек/	8			2			2	Конспект
	«Открытая система R3; архитектура «клиент-сервер»; масштабируемость системы R3» /Лаб/	8				6		2	Защита ЛР
2.1.	Цели создания АС. Место АС в информационном комплексе. Базовые принципы АС. Основные архитектурные решения проекта и структура АС производственного назначения. /Лек/	8			2			2	Конспект
2.2	«Базовые принципы АС. Основные архитектурные решения проекта и структура АС производственного назначения»/Лр/	8				6		1	Защита ЛР
	Раздел 2. Концептуальные аспекты защиты информации и обеспечения информационной безопасности в АС	8							
	Объекты ИБ. Основные угрозы ИБ. Описание общей структуры подсистемы защиты информации АС. Взаимодействие структурных подразделений по вопросам ИБ АС /Лек/	8			4			1	Конспект
	АС. защита информации на сетевом уровне /Лр/	8				8	1	1	Защита ЛР
	Принципы построения и функционирования межсетевых экранов. Фильтрация трафика; выполнение функций посредничества. Классификация межсетевых экранов. Фильтрующий маршрутизатор; шлюз сеансового уровня модели 0SI/1S0. /Лек/	8			2			2	Конспект
	Межсетевой экран Cisco PIX Firewall /Лр/	8				4		2	Защита ЛР
	Идентификация и подтверждение подлинности абонентов корпоративной сети. Протоколы взаимной проверки подлинности объектов /Лек/	8			2			2	Конспект
	«Протоколы взаимной проверки подлинности объектов» /Лаб/	8				4		2	Защита ЛР
	ЭП на основе симметричных криптоалгоритмов. ЭП на основе асимметричных криптоалгоритмов. Алгоритм ЭП DSA. Алгоритм ЭП ГОСТ 3 34.10-2001. Алгоритм хеширования SHA-2. /Лек/	8						2	Конспект
	Отечественный стандарт хеширования /Лр/	8				4		1	Защита ЛР
	Варианты создания защищенных виртуальных каналов. Протоколы VPN. Протоколы канального,	8			2			1	Конспект

	сетевого и сеансового уровней. Средства создания VPN /Лек/								
	Средства создания VPN /Лр/	8				4		1	Защита ЛР
	Общая характеристика СБД АС. RACF как средство доступа к наборам данных и ресурсам систем /Лек/	8			4			1	
	RACF как средство доступа к наборам данных и ресурсам систем /Лр/	8				4		1	Защита ЛР
	Основные типы вредоносного программного обеспечения. Организация антивирусной защиты /Лек/	8			2			2	Конспект
4.0	зачет		97		22	44		29	Тестирование

Объем самостоятельной 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.)		
8	Проработка лекционного материала по теме «Требования к АС. Концептуальные аспекты защиты информации и обеспечения информационной безопасности в АС»	Работа с книгой и конспектом, подготовка отчета по лабораторной работе	1-3 неделя	4	Устный опрос	Из списка литературы, конспект
8	Подготовка к лабораторной работе по теме «Открытая система R3; архитектура «клиент-сервер»; масштабируемость системы R3»»	Работа с книгой и конспектом, подготовка отчета по практической работе	3-4 неделя	4	Устный опрос	Из списка литературы, конспект
8	Подготовка к лабораторной работе по теме «Протоколы взаимной проверки подлинности объектов»»	Работа с книгой и конспектом, подготовка отчета по практической работе	5-6 неделя	4	Устный опрос	Из списка литературы, конспект
8	Проработка лекционного материала по теме «ЭП на основе симметричных криптоалгоритмов. ЭП на основе асимметричных криптоалгоритмов. Алгоритм ЭП DSA. Алгоритм ЭП ГОСТ 3 34.10-2001. Алгоритм хеширования SHA-2.»	Работа с книгой и конспектом, подготовка отчета по практической работе	7-8 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.)		
8	Подготовка к лабораторной работе по теме «Отечественный стандарт хеширования»	Работа с книгой и конспектом, подготовка отчета по практической работе	9-11 неделя	4	Устный опрос	Из списка литературы, конспект
8	Проработка лекционного материала по теме «Варианты создания защищенных виртуальных каналов. Протоколы VPN. Протоколы канального, сетевого и сеансового уровней. Средства создания VPN »	Работа с книгой и конспектом, подготовка отчета по практической работе	12-14 неделя	4	Устный опрос	Из списка литературы, конспект
8	Подготовка к лабораторной работе по теме «Средства создания VPN»	Работа с книгой и конспектом, подготовка отчета по практической работе	15-16 неделя	4	Устный опрос	Из списка литературы, конспект
8	Подготовка к лабораторной работе по теме «RACF как средство доступа к наборам данных и ресурсам систем»	Работа с книгой и конспектом, подготовка отчета по практической работе	17-18 неделя	1	Устный опрос	Из списка литературы, конспект

4.3. Содержание учебного материала

Т 1. Введение.

Информационный контур управления. АС как объект управления. Эволюция АС. Требования к АС

Т2. АС оперативного управления. АС информационное, математическое и программное обеспечение

Т3. Цели создания АС. Место АС в информационном комплексе. Базовые принципы АС. Основные архитектурные решения проекта и структура АС производственного назначения

Т4. Объекты ИБ. Основные угрозы ИБ. Описание общей структуры подсистемы защиты информации АС. Взаимодействие структурных подразделений по вопросам ИБ АС

Т5. Принципы построения и функционирования межсетевых экранов. Фильтрация трафика; выполнение функций посредничества. Классификация межсетевых экранов. Фильтрующий маршрутизатор; шлюз сеансового уровня модели 0SI/1S0.

Т6. Идентификация и подтверждение подлинности абонентов корпоративной сети. Протоколы взаимной проверки подлинности объектов

Т7. ЭП на основе симметричных криптоалгоритмов. ЭП на основе асимметричных криптоалгоритмов. Алгоритм ЭП DSA. Алгоритм ЭП ГОСТ 3 34.10-2001. Алгоритм хеширования SHA-2

Т8. Варианты создания защищенных виртуальных каналов. Протоколы VPN. Протоколы канального, сетевого и сеансового уровней. Средства создания VPN

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;Т2.	Анализ теоретических аспектов защиты информации в автоматизированных системах	2		Письменный текущий контроль. Защита ЛР	ИДК$_{ПК2.1}$ ИДК$_{ПК2.2}$
2	Т2;Т3.	Исследование видов и источников информации подлежащих защите	2		Письменный текущий контроль. Защита ЛР	ИДК$_{ПК2.1}$ ИДК$_{ПК2.2.}$
3	Т3;Т4;	Исследование угроз и вероятных каналов утечки конфиденциальной информации в автоматизированных системах	2		Письменный текущий контроль. Защита ЛР	ИДК$_{ПК2.1}$ ИДК$_{ПК2.2}$
4	Т4;Т5.	Рассмотрение комплексного подхода к защите информации	2		Письменный текущий контроль.	ИДК$_{ПК2.1}$ ИДК$_{ПК2.2}$

		в информационной системе организации			Защита ЛР	
5	Т5;Т6.	Использование программно-технических методов защиты информации в автоматизированных системах	2		Письменный текущий контроль. Защита ЛР	$ИДК_{ПК2.1}$ $ИДК_{ПК2.2}$
6	Т6;Т7.	Инженерно-техническая защита информационных ресурсов	2		Письменный текущий контроль. Защита ЛР	$ИДК_{ПК2.1}$ $ИДК_{ПК2.2}$
7	Т7;Т8.	Основные виды специальных технических средств предназначенных негласного получения информации	2		Письменный текущий контроль. Защита ЛР	$ИДК_{ПК2.1}$ $ИДК_{ПК2.2}$
8	Т2;Т4.	Анализ функций и свойств информационных технологий в механизме преступлений против информационной безопасности	2		Письменный текущий контроль. Защита ЛР	$ИДК_{ПК2.1}$ $ИДК_{ПК2.2}$
9	Т3;Т5.	Анализ видов правонарушений в сфере информации, информационных технологий и защиты информации	2		Письменный текущий контроль. Защита ЛР	$ИДК_{ПК2.1}$ $ИДК_{ПК2.2}$
10	Т4;Т7.	Обзор способов и механизмов преступлений в сфере информационной безопасности	2		Письменный текущий контроль. Защита ЛР	$ИДК_{ПК2.1}$ $ИДК_{ПК2.2}$
11	Т6,Т8.	Анализ особенностей характеристики личности компьютерных преступников	2		Письменный текущий контроль. Защита ЛР	$ИДК_{ПК2.1}$ $ИДК_{ПК2.2}$
11	Т2;Т7.	Методы поиска и фиксации электронных следов правонарушений в	2		Письменный текущий контроль. Защита ЛР	$ИДК_{ПК2.1}$ $ИДК_{ПК2.2}$

		информационных системах				
13	Т2;Т6.	Типичные ошибки, допускаемые при фиксации фактов нарушений сфере информационной безопасности	2		Письменный текущий контроль. Защита ЛР	ИДК$_{ПК2.1}$ ИДК$_{ПК2.2}$
14	Т4;Т7.	Анализ негативных последствий несанкционированного доступа к защищаемой компьютерной информации	2		Письменный текущий контроль. Защита ЛР	ИДК$_{ПК2.1}$ ИДК$_{ПК2.2}$
15	Т5;Т8.	Особенности организации работы с персоналом, имеющим доступ к конфиденциальной информации	2		Письменный текущий контроль. Защита ЛР	ИДК$_{ПК2.1}$ ИДК$_{ПК2.2}$
16	Т3;Т7.	Роль полиграфа в обеспечении защиты информации при осуществлении кадровой работы организации	7		Письменный текущий контроль. Защита ЛР	ИДК$_{ПК2.1}$ ИДК$_{ПК2.2}$
17	Т2;Т4.	Исследование информационно-технологических средств и приемов противодействия установлению правонарушителей в сфере информационной безопасности	7		Письменный текущий контроль. Защита ЛР	ИДК$_{ПК2.1}$ ИДК$_{ПК2.2}$

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	Т1. АС оперативного управления. АС информационное,	Осмысление материала лекций. Подготовка к	ПК-2	ИДК$_{ПК2.1}$ ИДК$_{ПК2.2}$

	математическое и программное обеспечение	Л.Р.1.		
2.	Т2. Цели создания АС. Место АС в информационном комплексе. Базовые принципы АС. Основные архитектурные решения проекта и структура АС производственного назначения	Осмысление материала лекций. Подготовка к Л.Р.	ПК-2 ПК-3	$ИДК_{ПК2.1}$ $ИДК_{ПК2.2}$ $ИДК_{ПК3.1}$
3.	Т3. Объекты ИБ. Основные угрозы ИБ. Описание общей структуры подсистемы защиты информации АС. Взаимодействие структурных подразделений по вопросам ИБ АС	Осмысление материала лекций. Подготовка к Л.Р.	ПК-2 ПК-3	$ИДК_{ПК2.1}$ $ИДК_{ПК2.2}$ $ИДК_{ПК3.1}$
4.	Т4. Принципы построения и функционирования межсетевых экранов. Фильтрация трафика; выполнение функций посредничества. Классификация межсетевых экранов. Фильтрующий маршрутизатор; шлюз сеансового уровня модели 0SI/1S0.	Осмысление материала лекций. Подготовка к Л.Р.	ПК-2 ПК-3	$ИДК_{ПК2.1}$ $ИДК_{ПК2.2}$ $ИДК_{ПК3.1}$
5.	Т5. Идентификация и подтверждение подлинности абонентов корпоративной сети. Протоколы взаимной проверки подлинности объектов	Осмысление материала лекций. Подготовка к Л.Р.	ПК-2 ПК-3	$ИДК_{ПК2.1}$ $ИДК_{ПК2.2}$ $ИДК_{ПК3.1}$
6.	Т6. ЭП на основе симметричных криптоалгоритмов. ЭП на основе асимметричных криптоалгоритмов. Алгоритм ЭП DSA. Алгоритм ЭП ГОСТ 3 34.10-2001. Алгоритм хеширования SHA-2	Осмысление материала лекций. Подготовка к Л.Р.	ПК-2 ПК-3	$ИДК_{ПК2.1}$ $ИДК_{ПК2.2}$ $ИДК_{ПК3.1}$
7.	Т7. Варианты создания защищенных виртуальных каналов. Протоколы VPN. Протоколы канального, сетевого и сеансового	Осмысление материала лекций. Подготовка к Л.Р.	ПК-2	$ИДК_{ПК2.1}$ $ИДК_{ПК2.2}$

	уровней. Средства создания VPN			
8.	Т8. АС оперативного управления. АС информационное, математическое и программное обеспечение	Осмысление материала лекций. Подготовка к ЛР.	ПК-2 ПК-3	$ИДК_{ПК2.1}$ $ИДК_{ПК2.2}$ $ИДК_{ПК3.1}$

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:

Т1. АС оперативного управления. АС информационное, математическое и программное обеспечение

Т2. Цели создания АС. Место АС в информационном комплексе. Базовые принципы АС. Основные архитектурные решения проекта и структура АС производственного назначения

Т3. Объекты ИБ. Основные угрозы ИБ. Описание общей структуры подсистемы защиты информации АС. Взаимодействие структурных подразделений по вопросам ИБ АС

Т4. Принципы построения и функционирования межсетевых экранов. Фильтрация трафика; выполнение функций посредничества. Классификация межсетевых экранов. Фильтрующий маршрутизатор; шлюз сеансового уровня модели 0SI/1S0.

Т5. Идентификация и подтверждение подлинности абонентов корпоративной сети. Протоколы взаимной проверки подлинности объектов

Т6. ЭП на основе симметричных криптоалгоритмов. ЭП на основе асимметричных криптоалгоритмов. Алгоритм ЭП DSA. Алгоритм ЭП ГОСТ 3 34.10-2001. Алгоритм хеширования SHA-2

Т7. Варианты создания защищенных виртуальных каналов. Протоколы VPN. Протоколы канального, сетевого и сеансового уровней. Средства создания VPN

Т8. АС оперативного управления. АС информационное, математическое и программное обеспечение

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. Рябов, И. В. Автоматизированные информационно-управляющие системы : учебное пособие / И. В. Рябов. Йошкар-Ола : Поволжский государственный технологический университет, 2015. - 200с. - Текст: электронный. - URL: https://biblioclub.ru/index.php?page=book&id=439330 (дата обращения: 14.09.2022)

2. Шишов, О. В. Современные средства АСУ ТП : учебник / О. В. Шишов. Москва, Вологда : Инфра-Инженерия, 2021. - 532с. - Текст: электронный. - URL: https://biblioclub.ru/index.php?page=book&id=617234 (дата обращения: 14.09.2022)

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	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 .

		достаточно полно отвечает на дополнительные вопросы.		

Вопросы для письменного текущего контроля приведены ниже:

1. Основные направления развития АС
2. Схемы автоматизированной системы управления
3. Основные виды АС.
4. RACF как средство доступа к наборам данных и ресурсам систем.
5. Основные типы вредоносного программного обеспечения.
6. Информационный контур управления.
7.АС как объект управления.
8. Эволюция АС. Требования к АС
9. АС оперативного управления. АС информационное, математическое и программное обеспечение.
10. Цели создания АС.
11. Место АС в информационном комплексе.
12. Базовые принципы АС.
13. Основные архитектурные решения проекта и структура АС производственного назначения.
14. Ландшафт вычислительной системы.
15. Возможности развития системы АС.
16. Повышение защищенности информационных ресурсов АС от злонамеренного использования или разрушения).

Перечень примерных вопросов для защиты практических работ:

ЛР1. Информационный контур управления. АС как объект управления. Эволюция АС. Требования к АС.

ЛР2. АС оперативного управления. АС информационное, математическое и программное обеспечение.

ЛР3. Цели создания АС. Место АС в информационном комплексе. Базовые принципы АС. Основные архитектурные решения проекта и структура АС производственного назначения

ЛР4. Объекты ИБ. Основные угрозы ИБ. Описание общей структуры подсистемы защиты информации АС. Взаимодействие структурных подразделений по вопросам ИБ АС

ЛР5. Принципы построения и функционирования межсетевых экранов. Фильтрация трафика; выполнение функций посредничества. Классификация межсетевых экранов. Фильтрующий маршрутизатор; шлюз сеансового уровня модели 0SI/1S0.

ЛР6. Идентификация и подтверждение подлинности абонентов корпоративной сети. Протоколы взаимной проверки подлинности объектов

ЛР7. ЭП на основе симметричных криптоалгоритмов. ЭП на основе асимметричных криптоалгоритмов. Алгоритм ЭП DSA. Алгоритм ЭП ГОСТ 3 34.10-2001. Алгоритм хеширования SHA-2

ЛР8. Варианты создания защищенных виртуальных каналов. Протоколы VPN. Протоколы канального, сетевого и сеансового уровней. Средства создания VPN

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 ПК-2 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

Образец типового итогового теста по дисциплине за весь период освоения:

Вариант 1

1. Что понимается под конфиденциальностью информации?

   А).Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

   Б). Ограничение доступа к информации третьих лиц.

   В). Информация доступ к которой ограничен.

2. Кем является обладатель информации согласно Закону об информации?

   А). Лицо самостоятельно создавшее информацию

   Б). Лицо получившее информацию на законных основаниях.

   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. Руководящий документ по реализации обязательных мероприятий при проведении работ по защите информации в АСУ:

   А. Приказ ФСТЭК России N 21;

Б. Приказ ФСТЭК России N 17;
В. Приказ ФСТЭК России N 31.

4. Требования к проведению работ по защите информации в АСУ

А. Формирование требований к защите информации в автоматизированной системе управления производственными и технологическими процессами; разработка системы защиты автоматизированной системы управления; внедрение системы защиты автоматизированной системы управления;

Б. Аттестация автоматизированной системы;

В. Лицензирование.

5. Руководящий документ для моделирования угроз ИБ:
А. Методика оценки угроз безопасности информации» Утвержден ФСТЭК России 5 февраля 2021;
Б. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (ФСТЭК России, 2008 г.);
В. Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры (ФСТЭК России, 2007г.).

9. Целью определения угроз безопасности информации является:

А. Установления потенциальных угроз безопасности;
Б. Установления потенциальных уязвимостей АС ТП;

В. Установление того, существует ли возможность нарушения конфиденциальности, целостности или доступности информации, содержащейся в информационной системе.

7. Защита и контроль web-трафика (Web Security)- состав, функции
А. Защита от шпионских программ, вредоносного мобильного кода, фишинга, ботов, и другие;
Б. Проверка подлинности пользователя;
В. Функции межсетевых экранов.

8. Сетевые системы предотвращения вторжений (Network IPS)- функции:

А. Функции межсетевых экранов;

Б. Анализа и контроля трафика;

В. Защита от шпионских программ, вредоносного мобильного кода.

9. Криптографические шлюзы (VPN) назначение:

А. Обеспечение защиты от вторжения со стороны сетей передачи данных (Интернет), обеспечения конфиденциальности при передаче информации по открытым каналам связи (VPN), а также организации безопасного доступа пользователей к ресурсам сетей общего пользования;

Б. Обеспечение аутентификации;

В. Настройки параметров безопасности операционной системы.

10. Модель угроз безопасности информации должна содержать:
а). краткое описание архитектуры значимого объекта, характеристику источников угроз безопасности информации, в том числе модель нарушителя, и описание всех угроз безопасности информации, актуальных для значимого объекта;
б). модель нарушителя, и описание всех угроз безопасности информации, актуальных для значимого объекта;
в). краткое описание архитектуры значимого объекта, характеристику источников угроз безопасности информации.

11. Системы безопасности должны обеспечивать:
а). восстановление функционирования системы безопасности информационной инфраструктуры;
б). недопущение воздействия на технические средства обработки информации, в результате которого может быть нарушено и (или) прекращено функционирование информационной инфраструктуры
в). устойчивое функционирование системы безопасности информационной инфраструктуры.

12. Категории информационных рисков:

А) Риски, вызванные утратой и/или утечкой информации и использованием ее конкурентами или сотрудниками в целях, которые могут повредить бизнесу;

Б) Риски технических сбоев работы каналов передачи информации, которые могут привести к убыткам;

В) Риски, вызванные форс-мажорными обстоятельствами.

13. Технические каналы утечки информации возникают:

А) При использовании злоумышленником специальных технических средств промышленного шпионажа, позволяющих получать защищаемую информацию при непосредственном контакте с персоналом фирмы, документами, делами и базами данных;

Б) При использовании злоумышленником специальных технических средств промышленного шпионажа, позволяющих получать защищаемую информацию без непосредственного контакта с персоналом фирмы, документами, делами и базами данных;

В) При использовании злоумышленником специальных технических средств для воздействия на средства защиты информации;

14. Целью анализа рисков является:
А) Оценка угроз и уязвимостей, возможного ущерба, учитывая уровень защищенности информационной системы;
Б) Проверка уровня защищенности информационной системы;

В) Оценка текущего состояния защищенности информационной системы

15. Угрозы безопасности информационным автоматизированным системам это:

А) Совокупность условий и факторов, которые могут стать причиной нарушения целостности, доступности, конфиденциальности информации;

Б) Совокупность условий и факторов, которые могут причинить ущерб информации;

В) Совокупность условий и факторов, которые могут стать причиной нарушения информации.

Вариант 2

1) Возможность за приемлемое время получить требуемую информационную услугу называется:

1. Конфиденциальность
2. Доступность
3. Целостность
4. Непрерывность

2) К аспектам информационной безопасности не относится:

1. Доступность
2. Целостность
3. Конфиденциальность
4. Защищенность

3) По каким критериям нельзя классифицировать угрозы:

1. по расположению источника угроз
2. по аспекту информационной безопасности, против которого угрозы направлены в первую очередь
3. по способу предотвращения
4. по компонентам информационных систем, на которые угрозы нацелены

4) Главное достоинство парольной аутентификации – …

1. простота
2. надежность
3. секретность
4. запоминаемость

5) Сколько уровней включает в себя сетевая модель OSI?

1. 5
2. 7
3. 6
4. 8

6) Межсетевой экран (Брандмауэр, firewall) – это…

1. Комплекс аппаратных средств
2. Комплекс программных средств

3. Комплекс аппаратных или программных средств
4. Комплекс аппаратных и программных средств

7) На каком уровне сетевой модели OSI не работает межсетевой экран:

1. Физический
2. Сеансовый
3. Сетевой
4. Транспортный

8) Межсетевого экрана какого класса не существует:

1. экранирующий маршрутизатор
2. экранирующий коммутатор
3. экранирующий транспорт
4. экранирующий шлюз

9) Что из перечисленного не входит в состав программного комплекса антивирусной защиты:

1. Подсистема сканирования
2. Подсистема управления
3. Подсистема обнаружения вирусной активности
4. Подсистема устранения вирусной активности

10) На каком этапе заканчивается жизненный цикл автоматизированной системы?

1. Бета-тестирование системы
2. Внедрение финальной версии системы в эксплуатацию
3. Прекращение сопровождения и технической поддержки системы
4. Альфа-тестирование системы

11) Какие задачи выполняет теория защиты информации:

1. предоставлять полные и адекватные сведения о происхождении, сущности и развитии проблем защиты
2. аккумулировать опыт предшествующего развития исследований, разработок и практического решения задач защиты информации
3. формировать научно обоснованные перспективные направления развития теории и практики защиты информации
4. выполняет все вышеперечисленные

12) Какой из протоколов не относится к протоколам защищенной передачи данных в сети Интернет:

1. SSL
2. SET
3. HTTP
4. IPSec

13) Какого метода разграничения доступа не существует:

1. разграничение доступа по спискам
2. разграничение доступа по уровням секретности и категориям
3. локальное разграничение доступа
4. парольное разграничение доступа

14) К основным функциям подсистемы защиты операционной системы относятся:

1. идентификация, аутентификация, авторизация, управление политикой безопасности и разграничение доступа
2. криптографические функции
3. сетевые функции
4. все вышеперечисленные

15) Риск – это…

1. вероятностная оценка величины возможного ущерба, который может понести владелец информационного ресурса в результате успешно проведенной атаки
2. фактическая оценка величины ущерба, который понес владелец информационного ресурса в результате успешно проведенной атаки
3. действие, которое направлено на нарушение конфиденциальности, целостности и/или доступности информации, а также на нелегальное использование других ресурсов сети
4. реализованная угроза

№	Вид контроля	Контролируемые темы (разделы)	Контролируемые компетенции/ индикаторы
1	**2**	**3**	**4**
1	Тестовое задание	Т1-Т8	ПК-2 ИДК$_{ПК2.1}$ ИДК$_{ПК2.2}$

Разработчики:

Доцент кафедры РФиРЭ _____ Серёдкин С.П.

Программа рассмотрена на заседании кафедры радиофизики и радиоэлектроники «27» февраля 2023 г. Протокол № 7

И.о.зав. кафедрой _____ Колесник С.Н.