ВОЕННО-КОСМИЧЕСКАЯ АКАДЕМИЯ ИМЕНИ А.Ф.МОЖАЙСКОГО

КАФЕДРА МАТЕМАТИЧЕСКОГО И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

ТЕМАТИЧЕСКИЙ ПЛАН
изучения дисциплины

Защита информации

г. Санкт-Петербург
202_ г.

УТВЕРЖДАЮ
Начальник 27 кафедры
полковник
С.Войцеховский
« _____ » _____ 202__ г.

Кафедра 27

ТЕМАТИЧЕСКИЙ ПЛАН

изучения дисциплины **Защита информации**

(наименование дисциплины (модуля))

по специальности **09.05.01 Применение и эксплуатация автоматизированных систем специального назначения**

(код и наименование специальности по ФГОС)

по специализации **Программное и математическое обеспечение систем управления летательными аппаратами**

(наименование специализации по ФГОС)

по военной специальности **Математическое, программное и информационное обеспечение вычислительной техники и автоматизированных систем**

(наименование специальности по КТ)

I. Распределение учебного времени по семестрам и видам учебных занятий

Семестры	Трудоемкость дисциплины (модуля), зач.ед /час.	Контактная работа обучающихся с преподавателем	В том числе														Время, отводимое на самостоятельную работу	Отчетность за изучение дисциплины (модуля)
			Лекции	Семинары	лабораторные работы	Практические занятия	Групповые упражнения	Групповые занятия	Тактические (тактико-специальные) занятия и учения	кшу, военные (военно-специальные) игры	контрольные работы (занятия)	Курсовые работы (проекты, задачи)	учебные занятия других видов	консультации	теоретические (научно-практические) конференции	Экзамены, зачеты		
7	***2,5/99***	***66***	***26***			***22***						***16***				***2***	***33***	***Защ.курс.***
8	***3,5/117***	***60***	***14***			***40***										***6***	***57***	***Экз.***
Итого	***6/216***	***126***	***40***			***62***						***16***				***8***	***90***	***Экз.***

II. План изучения дисциплины по видам учебных занятий

№ п/п	Виды учебных занятий	Кол-во часов	Наименование разделов и тем, учебные вопросы занятия	Материально-техническое и информационно-методическое обеспечение занятия	Задания на самостоятельную работу	
					Задание и литература (номер учебника или уч. пособия и номера страниц)	Время (в часах)
1	2	3	4	5	6	7
7 СЕМЕСТР						
		2	**Введение**			**1**
1	Лекция 1	2	***Вводная лекция*** 1. Предмет, цель и задачи дисциплины. Порядок изучения дисциплины. Литература. 2. Содержание предметной области защиты информации. 3. Основные положения доктрины информационной безопасности РФ.	ПЭВМ, видеопроектор, ПО MS PowerPoint.	Ознакомиться с предметом и задачами дисциплины. Изучить содержание системного подхода к защите ИПО, изучить доктрины РФ и США [20], [21], ГОСТ Р 50922, конспект лекций.	1
		8	**Раздел I. Основы защиты информации**			**4**
		2	**Тема 1. Сущность защиты информационно-программного обеспечения**			**1**
2	Лекция 2	2	***Классификация угроз и уязвимостей* информационно-программного обеспечения** 1. Основные определения. Сущность и цели защиты ИПО. 2. Классификация источников угроз. Классификация уязвимостей безопасности. Виды угроз ИПО. 3. Направления формализации процессов защиты информации. Матричные и многоуровневые модели доступа.	ПЭВМ, видеопроектор, ПО MS PowerPoint.	Изучить классификацию угроз и уязвимостей информационно-программного обеспечения. Изучить классификацию средств вычислительной техники и АС по уровням защищенности. [1], с. 30-50, 1310 – 1321, [3], с. 243-245, конспект лекций.	1
		6	**Тема 2. Основные документы по защите информации**			**3**
3	Лекция 3	2	***Основные документы по защите информации*** 1. Международные стандарты.	ПЭВМ, видеопроектор, экран, ПО.	Изучить основные документы по защите инфор-	1

№ п/п	Виды учебных занятий	Кол-во часов	Наименование разделов и тем, учебные вопросы занятия	Материально-техническое и информационно-методическое обеспечение занятия	Задания на самостоятельную работу	
					Задание и литература (номер учебника или уч. пособия и номера страниц)	Время (в часах)
1	2	3	4	5	6	7
			2. Законы РФ, указы Президента РФ, ГОСТЫ. 3. Документы ФСТЭК в области защиты информации.		мации. РД ФСТЭК [32]-[46], приказы МО РФ, ГОСТЫ, конспект лекций.	
4	Лекция 4	2	***Организация и обеспечение режима секретности на объектах информатизации ВС РФ*** 1. Основные руководящие документы по защите информации в МО РФ.	Приказы МО РФ по защите информации	Изучить основные положения приказов МО РФ по ЗИ ([47] - [50]), конспект лекций.	1
5	Лекция 5	2	***Лицензирование, сертификация и аттестация в области защиты информации как формы государственного регулирования применения информационных технологий*** 1. Лицензирование в области защиты информации. 2. Сертификация средств защиты информации. 3. Аттестация объектов информатизации.	ПЭВМ, видеопроектор, экран, ПО.	Изучить положение «По аттестации объектов информатизации по требованиям безопасности информации» ([37]), конспект лекций.	1
		106	**Раздел II. Методы и механизмы защиты информации**			**53**
		34	**Тема 3. Основные методы защиты информации**			**17**
6	Лекция 6	2	***Методы защиты информации*** 1. Понятие метода защиты информации и характеристика основных методов защиты информации. 2. Программно-аппаратные методы защиты информации.	ПЭВМ, видеопроектор, экран, ПО.	Ознакомиться с методами защиты информации. [4], с. 74-79, конспект лекций.	1
7	Курсовое проектирование 1	4	***Работа над индивидуальным заданием по созданию программного комплекса в соответствии с рекомендованной темой дипломного проекта***	ПЭВМ, видеопроектор, экран, ПО. РМ: Положение по организации КР (проекта), ГОСТы по	Литература в соответствии с темой, оформить требуемую сопроводительную документацию,	2

№ п/п	Виды учебных занятий	Кол-во часов	Наименование разделов и тем, учебные вопросы занятия	Материально-техническое и информационно-методическое обеспечение занятия	Задания на самостоятельную работу	
					Задание и литература (номер учебника или уч. пособия и номера страниц)	Время (в часах)
1	2	3	4	5	6	7
			1. Выдача курсантам тем курсовых работ. 2. Доведение положений руководства по оформлению курсовых работ.	созданию программного комплекса.	конспект лекций.	
8	Лекция 7	2	***Криптографические методы защиты информации*** 1. Основные понятия и определения. 2. Симметричные алгоритмы шифрования. Асимметричные алгоритмы шифрования. 3. Функции хеширования. Алгоритм электронно-цифровой подписи. Реализация криптографических методов зашиты информации.	ПЭВМ, видеопроектор, экран, ПО.	Изучить криптографические методы защиты информации. [4], с. 60-73, конспект лекций.	1
9	Лекция 8	2	***Стеганографические методы защиты информации*** 1. Введение в цифровую стеганографию. 2. Стеганографические методы защиты информации. Состав и основные принципы работы стегосистемы ЦВЗ. 3. Области применения стеганографии.	ПЭВМ, видеопроектор, экран, ПО.	Изучить криптографические методы ЗИ. [5], с. 28-40, конспект лекций.	1
10	Лекция 9	2	***Методы эталонных характеристик*** 1. Идентификация и аутентификация пользователей. 2. Защита программ и дистрибутивов от копирования. 3. Методы обнаружения модификации данных. Регистрация и анализ событий.	ПЭВМ, видеопроектор, экран, ПО.	Изучить методы эталонных характеристик. [6], с. 77-88, конспект лекций.	1
11	Лекция 10	2	***Защита программного обеспечения от несанкционированного копирования, исследования и модификации*** 1. Защита программ от копирования. 2. Защита программ от исследования. 3. Защита программ от модификаций.	ПЭВМ, видеопроектор, экран, ПО.	Изучить методы эталонных характеристик. [6], с. 77-88, конспект лекций.	

№ п/п	Виды учебных занятий	Кол-во часов	Наименование разделов и тем, учебные вопросы занятия	Материально-техническое и информационно-методическое обеспечение занятия	Задания на самостоятельную работу	
					Задание и литература (номер учебника или уч. пособия и номера страниц)	Время (в часах)
1	2	3	4	5	6	7
12	Практическое занятие 1	4	***Защита программных средств от несанкционированного копирования, исследования, модификации*** 1. Разработка программного модуля для защиты ПО от копирования. 2. Проверка работоспособности модуля путём установки его на любую программу. 3. Составление отчёта о проделанной работе, защита программы у преподавателя.	РМ ЭУ Скляров Д.В. Искусство защиты и взлома информации.	[6], с. 77-88, использовать интернет класс академии для поиска оригинальных решений по защите ПС от копирования, исследования, модификации. Конспект лекций.	2
13	Практическое занятие 2	4	***Защита программных средств от несанкционированного копирования, исследования, модификации*** 1. Разработка программного модуля для защиты ПО от исследования. 2. Проверка работоспособности модуля путём установки его на любую программу 3. Составление отчёта о проделанной работе, защита программы у преподавателя.	ПЭВМ, видеопроектор, экран, ПО.	Завершить разработку своего программного модуля для защиты ПО от копирования, используя интернет класс, конспект лекций.	2
14	Практическое занятие 3	4	***Защита программных средств от несанкционированного копирования, исследования, модификации*** 1. Разработка программного модуля для защиты ПО от модификации. 2. Проверка работоспособности модуля путём установки его на любую программу. 3. Составление отчёта о проделанной работе, защита программы у преподавателя.	ПЭВМ, видеопроектор, экран, ПО.	Завершить разработку своего программного модуля для защиты ПО от копирования и исследования, конспект лекций, подготовиться к рубежному контролю.	2
15	Практическое занятие 4	4	***Защита программных средств от несанкционированного копирования, исследования, модификации*** 1. Разработка программного модуля для за-	ПЭВМ, видеопроектор, экран, ПО. Вопросы для проведения рубежного кон-	Завершить разработку своего программного модуля для защиты ПО от копирования, исследова-	2

№ п/п	Виды учебных занятий	Кол-во часов	Наименование разделов и тем, учебные вопросы занятия	Материально-техническое и информационно-методическое обеспечение занятия	Задания на самостоятельную работу	
					Задание и литература (номер учебника или уч. пособия и номера страниц)	Время (в часах)
1	2	3	4	5	6	7
			щиты ПО от копирования, исследования и модификации. 2. Проверка работоспособности модулей путём установки их на любую программу. 3. Составление отчёта о проделанной работе, защита программ у преподавателя. 4. Рубежный контроль.	троля по теме № 1-4.	ния и модификации, конспект лекций.	
16	Курсовое проектирование 2	4	***Работа над индивидуальным заданием по созданию программного комплекса в соответствии с рекомендованной темой дипломного проекта***	ПЭВМ, видеопроектор, экран, ПО.	Литература в соответствии с рабочей программой дисциплины.	2
		42	**Тема 4. Программно-аппаратные средства защиты информации**			**21**
17	Лекция 11	2	***Программно-аппаратные средства защиты информации*** 1. Понятие и классификация средств защиты информации. 2. Характеристика средств разграничения доступа, вспомогательные программно-аппаратные средства.	ПЭВМ, видеопроектор, экран, ПО	Ознакомиться со средствами разграничения доступа. [5], с. 173-192 конспект лекций.	1
18	Лекция 12	2	***Средство защиты информации от несанкционированного доступа Secret Net»*** 1. Классификация и характеристики угроз безопасности информации, связанных с несанкционированным доступом 2. Архитектура, компоненты и защитные механизмы средства защиты информации от несанкционированного доступа Secret Net.	ПЭВМ, видеопроектор, экран, раздаточный материал, видеоматериал.	Изучить эксплуатационные документы «Методические рекомендации по настройке средства защиты информации от несанкционированного доступа Secret Net», [5], с. 192-220, [4], с. 22-42, конспект лекций.	1
19	Лекция 13	2	***Общие сведения о компьютерных вирусах***	ПЭВМ, видеопроектор,	Ознакомиться с основны-	1

№ п/п	Виды учебных занятий	Кол-во часов	Наименование разделов и тем, учебные вопросы занятия	Материально-техническое и информационно-методическое обеспечение занятия	Задания на самостоятельную работу	
					Задание и литература (номер учебника или уч. пособия и номера страниц)	Время (в часах)
1	2	3	4	5	6	7
			1. История появления компьютерных вирусов и факторы, влияющие на их распространение. 2. Понятие компьютерного вируса и основные этапы его жизненного цикла. 3. Наиболее распространённые компьютерные вирусы и их классификация.	экран, ПО.	ми этапами жизненного цикла вирусов. [5], с. 173-176, [4], с. 66-78. конспект лекций.	
23	Практическое занятие 5	4	***Администрирование средства защиты информации от несанкционированного доступа Secret Net*** 1. Установка средства защиты информации от несанкционированного доступа Secret Net. 2. Настройка учетных записей пользователей. 3. Настройка параметров политики безопасности.	ПЭВМ, видеопроектор, экран, ПО. РМ «Методика по настройке средства защиты информации от несанкционированного доступа Secret Net».	Изучить эксплуатационные документы «Методика по настройке средства защиты информации от несанкционированного доступа Secret Net», [5], с. 198-220, [4], с. 22-30.	2
24	Практическое занятие 6	2	***Администрирование средства защиты информации от несанкционированного доступа Secret Net*** 1. Настройка механизмов контроля целостности и замкнутой программной среды. 2. Настройка механизмов полномочного разграничения доступа.	ПЭВМ, видеопроектор, экран, ПО. РМ «Руководство по администрированию средства защиты информации от несанкционированного доступа Secret Net Secret Net».	Изучить эксплуатационные документы «Руководство по администрированию СЗИ от НСД Secret Net», [2], с. 192-220, [1], с. 30-42.	1
20	Курсовое проектирование 3	4	***Работа над индивидуальным заданием по созданию программного комплекса в соответствии с рекомендованной темой дипломного проекта***	ПЭВМ, видеопроектор, экран, ПО. РМ: Положение по организации КР (проекта), ГОСТы по созданию программного комплекса.	Литература в соответствии с темой, конспект лекций.	2
21	Курсовое	4	***Работа над индивидуальным заданием по со-***	ПЭВМ, видеопроектор,	Подготовить презентацию	2

№ п/п	Виды учебных занятий	Кол-во часов	Наименование разделов и тем, учебные вопросы занятия	Материально-техническое и информационно-методическое обеспечение занятия	Задания на самостоятельную работу	
					Задание и литература (номер учебника или уч. пособия и номера страниц)	Время (в часах)
1	2	3	4	5	6	7
	проектирование 4		***<u>зданию программного комплекса в соответствии с рекомендованной темой дипломного проекта</u>*** 1. Оформление курсовых работ.	экран, ПО. РМ: Положение по организации КР (проекта), ГОСТы по созданию программного комплекса.	и оформленную в соответствии с требованиями пояснительную записку, быть готовыми к защите своих курсовых работ.	
22	**Зачет курсовой работы**	2	**Защита курсовых работ**	ПЭВМ, видеопроектор, экран, ПО.		1
	Итого за семестр	66				33
8 СЕМЕСТР						
24	Практическое занятие 6	2	***<u>Работа с СЗИ от НСД Secret Net</u>*** 1. Настройка механизмов контроля целостности и замкнутой программной среды. 2. Настройка механизмов полномочного разграничения доступа.	ПЭВМ, видеопроектор, экран, ПО. РМ «Руководство по администрированию средства защиты информации от несанкционированного доступа Secret Net», задание на ПЗ № 2.	Изучить эксплуатационные документы «Руководство по администрированию средства защиты информации от несанкционированного доступа Secret Net», [5], с. 192-220, [4], с. 30-42.	1
23	Лекция 14	2	***<u>Организация антивирусной защиты</u>*** 1. Уровни защиты от компьютерных вирусов. 2. Общая характеристика сертифицированных антивирусных средств.	ПЭВМ, видеопроектор, экран, ПО.	Изучить эксплуатационный документ «Типовая инструкция по настройке средства антивирусной защиты Doctor Web», конспект лекций, [5], с. 66-78, 94-114.	1
29	Лекция 15	2	***<u>Межсетевые экраны</u>*** 1. Предназначение и классификация межсетевых экранов. 2. Схемы подключения сегментных межсете-	ПЭВМ, видеопроектор, экран, раздаточный материал.	[1], с. 665-713. [3], с. 296-300. [5], с. 42-66. конспект лекций.	1

№ п/п	Виды учебных занятий	Кол-во часов	Наименование разделов и тем, учебные вопросы занятия	Материально-техническое и информационно-методическое обеспечение занятия	Задания на самостоятельную работу	
					Задание и литература (номер учебника или уч. пособия и номера страниц)	Время (в часах)
1	2	3	4	5	6	7
			вых экранов и технология сетевой трансляции адресов. 3. Обзор современных межсетевых экранов.			
25	Практическое занятие 7	4	***Работа с антивирусным комплексом Doctor Web для Windows*** 1. Обнаружение и удаление компьютерных вирусов (тестовых) с ПЭВМ. 2. Обновление вирусных баз ПЭВМ.	ПЭВМ, видеопроектор, экран, ПО. РМ ЭД «Типовая инструкция по настройке средства АЗИ Doctor Web», конспект лекций.	Изучить эксплуатационный документ «Типовая инструкция по настройке средства АЗИ Doctor Web», конспект лекций.	2
26	Практическое занятие 8	4	***Работа с антивирусом Касперского для Windows*** 1. Обнаружение и удаление компьютерных вирусов (тестовых) с ПЭВМ. 2. Обновление вирусных баз ПЭВМ с магнитных носителей.	ПЭВМ, видеопроектор, экран, ПО. РМ «Руководство пользователя Касперского», «Методика обновления антивирусных баз».	Изучить эксплуатационный документ «Руководство пользователя Касперского», [1], с. 457-491. конспект лекций.	2
27	Практическое занятие 9	4	***Работа с межсетевым краном Agnitum Outpost FireWall*** 1. Освоить работу по настройке политики безопасности на ПЭВМ путём разрешения, запрещения доступа другим пользователям с помощью межсетевого крана.	ПЭВМ, видеопроектор, экран, ПО. РМ «Руководство по администрированию *Agnitum Outpost FireWall».*	Изучить ЭД «Руководство по администрированию *Agnitum Outpost FireWall,* [5], с. 42-66.	2
28	Практическое занятие 10	4	***Работа с средством анализа защищённости XSpider*** 1. Работа со сканером безопасности «XSPIDER». 2. Работа с TCP сервисами «XSPIDER». Перенаправление данных через TCP порт «XSPIDER». Работа IP пакетами «XSPIDER». 3. Составление отчёта о ходе выполнения	ПЭВМ, видеопроектор, экран, ПО. РМ «Руководство пользователя XSpider», «Индивидуальные задания».	Изучить ЭД «Руководство пользователя XSpider», конспект лекций, [5], с. 78-94.	2

№ п/п	Виды учебных занятий	Кол-во часов	Наименование разделов и тем, учебные вопросы занятия	Материально-техническое и информационно-методическое обеспечение занятия	Задания на самостоятельную работу	
					Задание и литература (номер учебника или уч. пособия и номера страниц)	Время (в часах)
1	2	3	4	5	6	7
			предыдущих заданий.			
		16	**Тема 5. Механизмы защиты ОС специального назначения**			**8**
30	Лекция 16	2	***Общие сведения об операционной системе МСВС 3.0*** 1. Общие сведения о реализации защиты ИПО в операционных системах. 2. Назначение состав и основные возможности ОС МСВС. 3. Основные задачи администратора системы (подключение пользователей, резервное копирование, мониторинг системы и др.)	ПЭВМ, видеопроектор, экран, ПО.	Изучить механизмы защиты ОС, конспект лекций, [4], с. 13-36. Быть готовым применить полученные знания на практическом занятии.	1
31	Лекция 17	2	***Система защиты от несанкционированного доступа ОС МСВС*** 1. Назначение, возможности и состав основного комплекса СЗИ ОС МСВС. *2.* Назначение, возможности и состав дополнительного комплекса СЗИ ОС МСВС.	ПЭВМ, видеопроектор, экран, ПО.	[5], с. 173-36. конспект лекций.	1
32	Лекция 18	2	***Система защиты от несанкционированного доступа ОС МСВС*** 1. Реализация защиты в комплексе «Система защиты от несанкционированного доступа. 2. Команды управления аудитом 3. Команды управления файлами пользователей и групп пользователей и восстановления файловой системы.	ПЭВМ, видеопроектор, экран, ПО.	Изучить основные механизмы защиты ОС МСВС, конспект лекций, [5], с. 114-121.	1
33	Практическое занятие 11	4	***Система контроля целостности Aide операционной системы МС ВС 3.0*** 1. Настройка и работа с системой контроля целостности Aide в ОС МС ВС 3.0.	ПЭВМ, видеопроектор, экран, ПО.	Повторить основные команды ОС МСВС. Изучить принципы организации защиты от НСД.	2

№ п/п	Виды учебных занятий	Кол-во часов	Наименование разделов и тем, учебные вопросы занятия	Материально-техническое и информационно-методическое обеспечение занятия	Задания на самостоятельную работу	
					Задание и литература (номер учебника или уч. пособия и номера страниц)	Время (в часах)
1	2	3	4	5	6	7
			2. Создание скрипта для автоматизации запуска процесса проверки.		[4], 114-120, [5], с. 121-134 конспект лекций.	
34	Практическое занятие 12	6	***Архивация и восстановление данных в ОС МС ВС 3.0*** 1. Установка и настройка средства управления резервным копированием КСЗИ СВАС. 2. Немедленная и плановая архивация данных в ОС МС ВС 3.0. 3. Восстановление данных в ОС МС ВС 3.0 с помощью средства управления резервным копированием КСЗИ СВАС. 4. Архивация и восстановление данных в ОС МС ВС 3.0 с помощью программы gzip, tar.	ПЭВМ, видеопроектор, экран, ПО.	Изучить принципы организации защиты от НСД. [5], с. 173-220, 323-351 конспект лекций. Быть готовым применить полученные знания на практическом занятии.	2
		14	**Тема 6. Комплексное обеспечение информационной безопасности АС**			**7**
36	Лекция 19	2	***Комплексное обеспечение информационной безопасности АС*** 1. Принципы построения комплексной системы информационной безопасности объекта. 2. Порядок разработки комплексной системы обеспечения информационной безопасности объекта. 3. Основные этапы создания системы информационной безопасности. 4. План мероприятий по защите служебной или коммерческой тайны. 5. Организационные меры обеспечения защиты информации.	ПЭВМ, видеопроектор, экран, ПО.	[5], с. 173-220, 323-351 [1], с. 82-101, конспект лекций.	1
38	Практическое	4	***Особенности работы с ПО РМ АОБИ «Си-***	ПЭВМ, видеопроектор,	Изучить работу анализа-	2

№ п/п	Виды учебных занятий	Кол-во часов	Наименование разделов и тем, учебные вопросы занятия	Материально-техническое и информационно-методическое обеспечение занятия	Задания на самостоятельную работу	
					Задание и литература (номер учебника или уч. пособия и номера страниц)	Время (в часах)
1	2	3	4	5	6	7
	занятие 13		***стема защиты от НСД» ОС МСВС 3.0***. 1. Установка сервера и агента домена безопасности ОС МСВС 3.0. 2. Включение АРМ клиентов ПО РМ АОБИ и пользователей в домен безопасности МСВС 3.0	экран, ПО.	торов исходных текстов программ и дизассемблеров, [1], с. 4-121, [2], с. 173-220, 323-351, конспект лекций	
37	Практическое занятие 14	4	***Проектирование системы комплексного обеспечения информационной безопасности АС*** 1. Разработка плана используемых ресурсов и средств для обеспечения информационной безопасности АС. 2. Настройка используемых программных средств обеспечения информационной безопасности АС. 3. Составление отчёта о проделанной работе.	ПЭВМ, видеопроектор, экран, ПО.	Доработать отчет, конспект лекций.	2
39	Практическое занятие 15	4	***Инструментальные средства обеспечения сертификационных испытаний программного обеспечения на отсутствие не декларированных возможностей*** 1. Установка программного средства IDA Pro. *2.* Дизассемблирование программ, имеющих (не имеющих) программные модули защиты с помощью IDA Pro.	ПЭВМ, видеопроектор, экран, ПО.	Изучить материалы конспекта лекций.	1
		2	**Заключение**			**1**
40	Лекция 20	2	***Перспективы и тенденции развития защиты информации*** 1. Краткий обзор дисциплины. 2. Проблемы обеспечения информационной безопасности отечественных информационных систем.	ПЭВМ, видеопроектор, экран, ПО.	Изучить «Концепцию развития системы управления ВС РФ на период до 2025 года», готовиться к сдаче экзамена по конспекту лекций	1

№ п/п	Виды учебных занятий	Кол-во часов	Наименование разделов и тем, учебные вопросы занятия	Материально-техническое и информационно-методическое обеспечение занятия	Задания на самостоятельную работу	
					Задание и литература (номер учебника или уч. пособия и номера страниц)	Время (в часах)
1	2	3	4	5	6	7
			3. Перспективы и тенденции развития.		и указанной в РП литературе.	
41	Экзамен	6				30
	Всего проведено часов учебных занятий	**216**				90
	из них:					
	лекции	40				
	практические занятия	62				
	Курсовые работы	16				
	Зачет курсовой работы	2				
	Экзамен	6				

III. Учебно-методическое и информационное обеспечение учебной дисциплины

1. Учебная Литература

Основная:

1. Информационная безопасность: – учебное пособие / В.М.Зима, СПб.: ВКА имени А.Ф.Можайского, 2017.
2. Криптографические методы защиты информации: - учебное пособие / А.Романченко СПб.: ВКА имени А.Ф.Можайского, 2016.

Дополнительная:

3. Принципы построения и функционирования аппаратно-программных средств телекоммуникационных систем. Часть2. Сетевые операционные системы и принципы обеспечения информационной безопасности в сетях / С.И. Макаренко, А.А. Ковальский, С.А.Краснов СПб.: Наукоемкие технологии 2020. – 357.
4. Войцеховский С.В., Воробьёв Е.Г. Методы и средства защиты компьютерной информации: учебно-методическое пособие. – СПб.: ВКА имени А.Ф. Можайского 2013. – 134 с.

5. Войцеховский С.В., Калиниченко С.В.. Архитектура и программное обеспечение современных компьютерных систем и сетей войск ВКО: учебно-методическое пособие. – СПб.: ВКА имени А.Ф. Можайского 2013. – 352 с.
6. Криптографические методы защиты информации: - практикум / М.А.Еремеев СПб.: ВКА имени А.Ф.Можайского, 2016.
7. Криптографические протоколы: - учебное пособие / М.А. Еремеев, Н.А. Молдовян, С.В. Пилькевич СПб.: ВКА имени А.Ф.Можайского, 2016.
8. Теоретико-числовые методы в криптографии: - практикум / М.А.Еремеев СПб.: ВКА имени А.Ф.Можайского, 2016.
9. Элементы криптоанализа: - учебное пособие / М.А.Еремеев , А.Романченко СПб.: ВКА имени А.Ф.Можайского, 2016.
10. Воробьев Е.Г. Защита информации в автоматизированных системах военного назначения. Учебное пособие – СПб, ВКА им.А.Ф. Можайского, 2007. – 252 с.
11. Вихорев С.В. Классификация угроз информационной безопасности. – http://www2.cnews.ru/comments/security/elvis_class.shtml
12. Краснов, С.А. Обзор моделей поиска и методов тематического анализа текстовой информации. // Компьютерные технологии и информационные системы. Сборник научных трудов. ВА ВПВО ВС РФ. 2011. Выпуск 20. С. 35-42.
13. Краснов, С.А. Выявление противоречий в семантически близкой информации на основе латентно-семантического анализа / С.А. Краснов, А.Д. Хомоненко, В.Л. Дашонок // Сборник научных трудов СПбГПУ «Проблемы информационной безопасности. Компьютерные системы» 2014. № 2. С. 73-84.
14. Хомоненко, А.Д. Применение методов латентно-семантического анализа для автоматической рубрикации документов / А.Д. Хомоненко, С.А. Краснов // Известия Петербургского университета путей сообщения. 2012. Вып. 2(31) С. 124-132.

Международные стандарты:

15. Международный стандарт ISO/IEC 17799:2000 (BS 7799-1) "Управление информационной безопасностью - Информационные технологии. - Information technology- Information security management".
16. Международный стандарт "Общие критерии безопасности информационных технологий" (ОК) ISO/IEC 15408.

Государственные стандарты РФ:

17. ГОСТ Р 50922-96 Защита информации. Основные термины и определения. Дата введения 1.07.97 г.
18. ГОСТ РВ 51987-2002 Типовые требования и показатели качества функционирования информационных систем. Дата введения 1.07.2003 г.
19. ГОСТ Р 51275-1999 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.
20. ГОСТ Р 51583-2000 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие

положения.

21. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования.

Руководящие документы:

22. Доктрина «Информационной безопасности РФ» Введена указом президента № 646 от 5 декабря 2016 г.
23. Военная доктрина РФ от 25 декабря 2014 г.
24. Федеральный закон «О лицензировании отдельных видов деятельности» от 08.08.2001 г. № 128.
25. ФЗ РФ «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года № 149-ФЗ.
26. ФЗ РФ «О государственной тайне» от 21 июля 1993 года.
27. ФЗ РФ № 152 «О персональных данных» от 27 июля 2006 года, ред. от 31.12.2017 г.
28. Указ Президента РФ «О мерах по обеспечению информационной безопасности РФ при использовании ИТКС международного информационного обмена» от 17 марта 2008 г.
29. Указ Президента РФ «Об утверждении Перечня сведений конфиденциального характера» от 6 марта 1997 г., в ред. от 13.07.2015 г.
30. Указ Президента РФ «Об утверждении Перечня сведений, отнесенных к государственной тайне» от 30 ноября 1995 г.
31. Указ Президента РФ «О стратегии национальной безопасности РФ до 2020 года» от 12 мая 2009 года.
32. Приказ ФСТЭК России «Об утверждении требований к обеспечению защиты информации в АСУ производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также на объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» от 14 марта 2014 года.
33. Совместный приказ ФСТЭК России, ФСБ России и Минком связи России «Об утверждении Порядка проведения классификации информационных систем персональных данных» от 31 декабря 2013 г.
34. Приказ ФСТЭК России «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» от 18 февраля 2013 года.
35. Приказ ФСТЭК России «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» от 11 февраля 2013 года.
36. Приказ ФСТЭК России «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования» от 31 августа 2010 года.
37. Положение «По аттестации объектов информатизации по требованиям безопасности информации» от 25 ноября 1994 г.
38. Методический документ «Меры защиты информации в государственных информационных системах» утвержден ФСТЭК России 11 февраля 2014 года.

39. Руководящий документ. Приказ председателя Гостехкомиссии России «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий» от 19 июня 2002 года.
40. Руководящий документ. Приказ председателя Гостехкомиссии России «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия не декларированных возможностей» от 4 июня 1999 года.
41. Руководящий документ. Приказ председателя Гостехкомиссии России «Средства вычислительной техники. Межсетевые экраны. Защита от НСД. Показатели защищенности от НСД к информации» от 25 июня 1997 года.
42. Руководящий документ. Приказ председателя Гостехкомиссии России «Автоматизированные системы. Защита от НСД к информации. Классификация АС и требования по защите информации» от 30 марта 1992 года.
43. Руководящий документ. Приказ председателя Гостехкомиссии России «Средства вычислительной техники. Защита от НСД к информации. Показатели защищенности от НСД к информации» от 30 марта 1992 года.
44. Руководящий документ. Приказ председателя Гостехкомиссии России «Защита от НСД к информации. Термины и определения» от 30 марта 1992 года.
45. Руководящий документ. Приказ председателя Гостехкомиссии России «Концепция защиты средств вычислительной техники и АС от НСД к информации» от 30 марта 1992 года.
46. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). ФСТЭК России, 2008 год

Приказы Министра обороны:

47. Приказ Министра обороны Российской Федерации № 010 от 2018 г.
48. Приказ Министра обороны Российской Федерации № 011 от 2013 г.
49. Приказ Министра обороны Российской Федерации № 080 от 2019 года.
50. Приказ Министра обороны Российской Федерации № 311 дсп от 5 июня 2019 г.
51. Приказ Министра обороны Российской Федерации № 1313 от 2010 г об утверждении «Инструкции о порядке допуска к государственной тайне».
52. Министра обороны Российской Федерации № 950 дсп от 19 апреля 2012 г об утверждении «Инструкции по организации ЗИ при подключении и использовании информационно-телекоммуникационных сетей общего пользования в … ».
53. Приказ Министра обороны Российской Федерации № 190 от 13.05.02 г. «О принятии на снабжение ВС РФ защищенных ОС МСВС 3.0, СУБД «Линтер-ВС» 6.0 и комплекса программных средств обеспечения повседневной деятельности должностных лиц КП «Офис» 1.0».
54. Приказ МО РФ № 392 от 2004 г. «О мерах по обеспечению информационной безопасности в ВС РФ при использовании

международных сетей (Интернет)».
Приказ Командующего Войсками ВКО «Об утверждении Инструкции по порядку применения машинных…» от 30 апреля 2013 года.

2.Программное обеспечение и информационно-справочные системы

- Операционная система Microsoft Windows 7 Professional.
- Операционная система МСВС 3.0
- Windows Media Player.
- Microsoft OfficeWord.
- Microsoft Office Excel.
- Microsoft Power Point.
- Microsoft Access.
- САВЗ Касперский.
- САВЗ Doctor Web.
- СЗИ от НСД Secret Net.
- MathCad.

Информационно-справочные системы.

- Справка Microsoft Word.
- Справка Microsoft PowerPoint.

3.Интернет-ресурсы

1. Библиотека электронных ресурсов МГУ им. М.В. Ломоносова.
http://www.msu.ru/index.html
2. Военная литература
http://militera.lib.ru
3. Российская Государственная библиотека РГБ
http://www.rsl.ru
4. Большая научная библиотека
http://www.sci-lib.net/
5. Электронная библиотека учебников
http://studentam.net
6. Bibliophika. Электронная библиотека ГПИБ России
http://www.bibliofika.ru
7. Открытая русская электронная библиотека
http://orel.rsl.ru/
8. Федеральный портал «Российское образование»
http://www.edu.ru/

9. Федеральное государственное бюджетное учреждение «Федеральный институт промышленной собственности» http://new.fips.ru/podacha-zayavki/podacha-zayavki-na-registratsiyu-programmy-dlya-evm-ili-bazy-dannykh/
10. Научное издание «Труды Военно-космической академии имени А.Ф.Можайского» http://trudvka.ru/

IV. Организационно-методические рекомендации преподавателям по проведению каждого учебного занятия

Учебная дисциплина «Защита информации» состоит из следующих разделов.
1. Основы защиты информации.
2. Методы и механизмы защиты информации.

Дисциплина базируется на учебном материале дисциплин: математический анализ, информатика, операционные системы, программирование, ЭВМ и периферийные устройства, сети и телекоммуникации, базы данных, компьютерное моделирование, структуры и алгоритмы обработки данных, теории языков программирования и методы трансляции.

Основными видами занятий при изучении дисциплины являются лекции, практические занятия, самостоятельные занятия под руководством преподавателя, курсовая работа, а также занятия в часы самостоятельной подготовки.

Целями лекционных занятий являются:

- дать курсантам основные определения, теоретические положения дисциплины;
- сконцентрировать внимание курсантов на наиболее важных и сложных вопросах, связанных с организацией защиты информации на объектах вычислительной техники.

В конце каждой лекции рекомендуется давать курсантам задание на самостоятельную подготовку с целью самостоятельного изучения дополнительных документов по защите информации, книг и методических пособий.

Целями практических занятий являются:

закрепление теоретических знаний;

привитие навыков в решении задач по разработке программного обеспечения необходимого для обеспечения информационной безопасности АС специального назначения;

проверки усвоения курсантами основных положений разделов или тем, по которым проводятся занятия.

Комплекс задач, решаемых в ходе практических занятий, должен подкреплять изученный теоретический материал раздела (темы) дисциплины; содержание заданий должно побуждать обучающихся к осознанному их решению, развивать у них творческую инициативу, и, по возможности, учитывать специальность, по которой они обучаются.

В практические занятия включаются следующие элементы:

опрос по теоретическому материалу, знание которого требуется для решения задач по теме занятия, продолжительностью 15 мин.;

формулировка исходных данных задач преподавателем и выработку обучающимся основной идеи и последовательности их решения;

самостоятельное решение задач обучающимися, вызываемыми для этой цели преподавателем;

подведение итогов занятия с обобщением полученных результатов и выдачей задач для решения обучающимися в часы самостоятельной работы.

Курсовая работа по дисциплине «Защита информации» проводится с целью научить слушателей и курсантов самостоятельно применять полученные знания для обеспечения защиты информации на объектах ВТ, привить навыки самостоятельного проектирования, производства расчетов, проведения научных исследований и обоснования принимаемых решений, а также правильности оформления курсовых и научных работ. Выполнение курсовой работы проводится в часы, установленные расписанием учебных занятий с использование компьютерного класса кафедры и в часы самоподготовки. Текущий контроль выполнения курсовых работ осуществлять на каждом занятии, на последнем занятии курсанты защищают свои курсовые работы.

Самостоятельная работа по дисциплине «Защита информации» имеет целью закрепление и углубление полученных знаний и навыков, поиск и приобретение новых знаний, в том числе с использованием автоматизированных обучающих курсов (систем), а также выполнение учебных заданий, подготовку к предстоящим занятиям, зачетам и экзаменам.

Текущий контроль проводить в виде контрольных опросов перед проведением каждого вида занятия (включая лекции) и в течение аттестационных недель. При проведении практических занятий и лабораторных работ должны быть оценены 100 % присутствующих на занятиях курсантов.

Как отмечалось выше, лекции составляют основу теоретического обучения и должны давать систематизированные основы научных знаний по дисциплине.

В ходе лекций следует формировать у обучающихся теоретическую базу профессиональных и профессионально-специализированных компетенций.

После третьей и последующих лекций в соответствии с ними проводятся практические занятия в целях выработки практических умений и приобретения навыков в применении полученных знаний при решении практических задач.

В материалах лекции № 1 – Введение.

Изложить предмет и задачи дисциплины, порядок изучения дисциплины, литературу для самостоятельной работы. Коснуться содержания, сущности и целей предметной области защиты информации. В дальнейшем концентрировать внимание обучающихся на наиболее сложных и узловых вопросах.

Лекция № 2 – Классификация угроз и уязвимостей ИПО.

Материал лекции должен содержать и раскрывать суть рассматриваемых учебных вопросов. В начале занятия провести контрольный опрос для контроля усвоения материала предыдущей лекции. С целью повышения наглядности на лекции целесообразно использовать: презентации, плакаты, раздаточный материал. Лектор должен разъяснить курсантам особенности изучения каждого учебного вопроса. Обратить внимание на:

Базовые понятия и определения. Классификация источников угроз. Классификация уязвимостей безопасности. Виды угроз ИПО. Направления формализации процессов защиты информации. Матричные и многоуровневые модели доступа.

Лекция № 3 – Основные документы по защите информации.

Материал лекции должен содержать и раскрывать суть рассматриваемых учебных вопросов. В начале занятия провести контрольный опрос для контроля усвоения материала предыдущей лекции. С целью повышения наглядности на лекции целесообразно

использовать: презентации, плакаты, раздаточный материал. Лектор должен разъяснить курсантам особенности изучения каждого учебного вопроса. Обратить внимание на:

Международные стандарты. Законы РФ, указы Президента РФ, ГОСТЫ. Документы ФСТЭК в области защиты информации.

Лекция № 4 – Организация и обеспечение режима секретности на объектах ВТ ВС РФ.

Материал лекции должен содержать и раскрывать суть рассматриваемых учебных вопросов. В начале занятия провести контрольный опрос для контроля усвоения материала предыдущей лекции. С целью повышения наглядности на лекции целесообразно использовать: презентации, плакаты, раздаточный материал. Лектор должен разъяснить курсантам особенности изучения каждого учебного вопроса. Обратить внимание на:

Основные руководящие документы по защите информации в МО РФ.

Лекция № 5 – Лицензирование, сертификация и аттестация в области защиты информации как формы государственного регулирования применения информационных технологий.

Материал лекции должен содержать и раскрывать суть рассматриваемых учебных вопросов. В начале занятия провести контрольный опрос для контроля усвоения материала предыдущей лекции. С целью повышения наглядности на лекции целесообразно использовать: презентации, плакаты, раздаточный материал. Лектор должен разъяснить курсантам особенности изучения каждого учебного вопроса. Обратить внимание на:

Лицензирование в области защиты информации. Сертификация средств защиты информации. Аттестация объектов информатизации.

Лекция № 6 – Методы защиты информации.

Материал лекции должен содержать и раскрывать суть рассматриваемых учебных вопросов. В начале занятия провести контрольный опрос для контроля усвоения материала предыдущей лекции. С целью повышения наглядности на лекции целесообразно использовать: презентации, плакаты, раздаточный материал. Лектор должен разъяснить курсантам особенности изучения каждого учебного вопроса. Обратить внимание на:

Понятие метода защиты информации и характеристика основных методов ЗИ. Программно-аппаратные методы ЗИ.

Лекция № 7 – Криптографические методы ЗИ

Материал лекции должен содержать и раскрывать суть рассматриваемых учебных вопросов. В начале занятия провести контрольный опрос для контроля усвоения материала предыдущей лекции. С целью повышения наглядности на лекции целесообразно использовать: презентации, плакаты, раздаточный материал. Лектор должен разъяснить курсантам особенности изучения каждого учебного вопроса. Обратить внимание на:

Основные понятия и определения. Симметричные алгоритмы шифрования. Асимметричные алгоритмы шифрования. Функции хеширования. Алгоритм ЭЦП. Реализация криптографических методов зашиты информации.

Лекция № 8 – Стеганографические методы ЗИ.

Материал лекции должен содержать и раскрывать суть рассматриваемых учебных вопросов. В начале занятия провести контрольный опрос для контроля усвоения материала предыдущей лекции. С целью повышения наглядности на лекции целесообразно

использовать: презентации, плакаты, раздаточный материал. Лектор должен разъяснить курсантам особенности изучения каждого учебного вопроса. Обратить внимание на:

Введение в цифровую стеганографию. Стеганографические методы защиты информации. Состав и основные принципы работы стегосистемы ЦВЗ. Области применения стеганографии.

Лекция № 9 – Методы эталонных характеристик

Материал лекции должен содержать и раскрывать суть рассматриваемых учебных вопросов. В начале занятия провести контрольный опрос для контроля усвоения материала предыдущей лекции. С целью повышения наглядности на лекции целесообразно использовать: презентации, плакаты, раздаточный материал. Лектор должен разъяснить курсантам особенности изучения каждого учебного вопроса. Обратить внимание на:

Идентификацию и аутентификацию пользователей. Защиту программ и дистрибутивов от копирования. Регистрацию и анализ событий. Методы обнаружения модификации данных.

Лекция № 10 – Защита программного обеспечения от несанкционированного копирования, исследования и модификации

Материал лекции должен содержать и раскрывать суть рассматриваемых учебных вопросов. В начале занятия провести контрольный опрос для контроля усвоения материала предыдущей лекции. С целью повышения наглядности на лекции целесообразно использовать: презентации, плакаты, раздаточный материал. Лектор должен разъяснить курсантам особенности изучения каждого учебного вопроса. Обратить внимание на:

Защита программ от копирования. Защита программ от исследования. Защита ПО от модификаций.

Практическое занятие № 1 – Защита программных средств от несанкционированного копирования, исследования, модификации.

В начале занятия произвести опрос курсантов по теоретическому материалу, знание которого требуется для решения задач по теме занятия. Продолжительность опроса – до 15 минут.

В случае, невозможности предоставления каждому курсанту индивидуальной ПЭВМ, работу проводить в составе утвержденных расчетов (в составе 2-х курсантов) по заданию. Выдать курсантам необходимые учебные материалы занятия и задания (каждый курсант должен получить и выполнить задание установку ОС). В ходе выполнения заданий дать команду на смену, чтобы оба члена расчета получили практические навыки. Использовать ПЭВМ под управлением ОС Microsoft Windows. Проверить результаты выполнения курсантами заданий, при необходимости задать дополнительные вопросы и оценить ответы обучающихся. Обратить внимание на:

Разработка программного модуля для защиты ПО от копирования. Проверка работоспособности модуля путём установки его на любую программу. Составление отчёта о проделанной работе, защита программы у преподавателя.

Практическое занятие № 2 – Защита программных средств от несанкционированного копирования, исследования, модификации.

В начале занятия произвести опрос курсантов по теоретическому материалу, знание которого требуется для решения задач по теме занятия. Продолжительность опроса – до 15 минут.

В случае, невозможности предоставления каждому курсанту индивидуальной ПЭВМ, работу проводить в составе утвержденных расчетов (в составе 2-х курсантов) по заданию. Выдать курсантам необходимые учебные материалы занятия и задания (каждый курсант должен получить и выполнить задание установку ОС). В ходе выполнения заданий дать команду на смену, чтобы оба члена расчета получили практические навыки. Использовать ПЭВМ под управлением ОС Microsoft Windows. Проверить результаты выполнения курсантами заданий, при необходимости задать дополнительные вопросы и оценить ответы обучающихся. Обратить внимание на:

Разработка программного модуля для защиты ПО от исследования. Проверка работоспособности модуля путём установки его на любую программу. Составление отчёта о проделанной работе, защита программы у преподавателя.

Курсовое проектирование № 1 – Работа над индивидуальным заданием по созданию программного комплекса в соответствии с рекомендованной темой дипломного проекта

Выдача курсантам тем курсовых работ. Доведение положений руководства по оформлению курсовых работ.

Практическое занятие № 3 – Защита программных средств от несанкционированного копирования, исследования, модификации.

В начале занятия произвести опрос курсантов по теоретическому материалу, знание которого требуется для решения задач по теме занятия. Продолжительность опроса – до 15 минут.

В случае, невозможности предоставления каждому курсанту индивидуальной ПЭВМ, работу проводить в составе утвержденных расчетов (в составе 2-х курсантов) по заданию. Выдать курсантам необходимые учебные материалы занятия и задания (каждый курсант должен получить и выполнить задание установку ОС). В ходе выполнения заданий дать команду на смену, чтобы оба члена расчета получили практические навыки. Использовать ПЭВМ под управлением ОС Microsoft Windows. Проверить результаты выполнения курсантами заданий, при необходимости задать дополнительные вопросы и оценить ответы обучающихся. Обратить внимание на:

Разработка программного модуля для защиты ПО от модификации. Проверка работоспособности модуля путём установки его на любую программу. Составление отчёта о проделанной работе, защита программы у преподавателя.

Практическое занятие № 4 – Защита программных средств от несанкционированного копирования, исследования, модификации.

В начале занятия произвести опрос курсантов по теоретическому материалу, знание которого требуется для решения задач по теме занятия. Продолжительность опроса – до 15 минут.

В случае, невозможности предоставления каждому курсанту индивидуальной ПЭВМ, работу проводить в составе утвержденных расчетов (в составе 2-х курсантов) по заданию. Выдать курсантам необходимые учебные материалы занятия и задания (каждый курсант должен получить и выполнить задание установку ОС). В ходе выполнения заданий дать команду на смену, чтобы оба члена расчета получили практические навыки. Использовать ПЭВМ под управлением ОС Microsoft Windows. Проверить результаты выполнения курсантами заданий, при необходимости задать дополнительные вопросы и оценить ответы обучающихся. Обратить внимание на:

Разработка программного модуля для защиты ПО от копирования, исследования и модификации. Проверка работоспособности модуля путём установки его на любую программу. Составление отчёта о проделанной работе, защита программы у преподавателя. Проведение **рубежного контроля** по пройденному материалу (Тема №1-4).

Курсовое проектирование № 2 – Работа над индивидуальным заданием по созданию программного комплекса в соответствии с рекомендованной темой дипломного проекта.

Курсовое проектирование № 3 – Работа над индивидуальным заданием по созданию программного комплекса в соответствии с рекомендованной темой дипломного проекта.

Курсовое проектирование № 4 – Работа над индивидуальным заданием по созданию программного комплекса в соответствии с рекомендованной темой дипломного проекта. Оформление курсовых работ.

Лекция № 11 – Программно-аппаратные средства ЗИ.

Материал лекции должен содержать и раскрывать суть рассматриваемых учебных вопросов. В начале занятия провести контрольный опрос для контроля усвоения материала предыдущей лекции. С целью повышения наглядности на лекции целесообразно использовать: презентации, плакаты, раздаточный материал. Лектор должен разъяснить курсантам особенности изучения каждого учебного вопроса. Обратить внимание на:

Понятие и классификация средств ЗИ. Краткая характеристика средств разграничения доступа (СРД). Вспомогательные программно-аппаратные средства.

Основные понятия и классификация вредоносного ПО. Программно-аппаратные средства и методы защиты компьютерной информации. Типовые средства защиты информации, применяемые в автоматизированных системах военного назначения (АС ВН).

Лекция № 12 – СЗИ от НСД Secret Net.

Материал лекции должен содержать и раскрывать суть рассматриваемых учебных вопросов. В начале занятия провести контрольный опрос для контроля усвоения материала предыдущей лекции. С целью повышения наглядности на лекции целесообразно использовать: презентации, плакаты, раздаточный материал. Лектор должен разъяснить курсантам особенности изучения каждого учебного вопроса. Обратить внимание на:

Угрозы информационной безопасности, связанные с НСД. Архитектура, компоненты и защитные механизмы системы СРД Secret Net. Аппаратная поддержка системы Secret Net.

Лекция № 13 – Межсетевые экраны.

Материал лекции должен содержать и раскрывать суть рассматриваемых учебных вопросов. В начале занятия провести контрольный опрос для контроля усвоения материала предыдущей лекции. С целью повышения наглядности на лекции целесообразно использовать: презентации, плакаты, раздаточный материал. Лектор должен разъяснить курсантам особенности изучения каждого учебного вопроса. Обратить внимание на:

Предназначение и классификация МЭ. Схемы подключения сегментных МЭ и технология сетевой трансляции адресов. Обзор современных МЭ.

Практическое занятие № 5 – Работа с СРД Secret Net и Соболь PCI.

В начале занятия произвести опрос курсантов по теоретическому материалу, знание которого требуется для решения задач по теме занятия. Продолжительность опроса – до 15 минут.

В случае, невозможности предоставления каждому курсанту индивидуальной ПЭВМ, работу проводить в составе утвержденных расчетов (в составе 2-х курсантов) по заданию. Выдать курсантам необходимые учебные материалы занятия и задания (каждый курсант должен получить и выполнить задание установку ОС). В ходе выполнения заданий дать команду на смену, чтобы оба члена расчета получили практические навыки. Использовать ПЭВМ под управлением ОС Microsoft Windows. Проверить результаты выполнения курсантами заданий, при необходимости задать дополнительные вопросы и оценить ответы обучающихся. Обратить внимание на:

Освоить работу по созданию новых пользователей и групп пользователей. Освоить работу системы контроля целостности.

Практическое занятие № 6 – Работа с СРД Secret Net и Соболь PCI.

Освоить работу по ведению аудита. Освоить работу по установке необходимых настроек в соответствии с дополнительными условиями сертификата на СРД. Освоить работу по способам управления разграничением доступа пользователей к информационно-программным ресурсам.

Защита курсовых работ – промежуточная аттестация.

Практическое занятие № 7 – Работа с МЭ Agnitum Outpost Fire Wall.

В начале занятия произвести опрос курсантов по теоретическому материалу, знание которого требуется для решения задач по теме занятия. Продолжительность опроса – до 15 минут.

В случае, невозможности предоставления каждому курсанту индивидуальной ПЭВМ, работу проводить в составе утвержденных расчетов (в составе 2-х курсантов) по заданию. Выдать курсантам необходимые учебные материалы занятия и задания (каждый курсант должен получить и выполнить задание установку ОС). В ходе выполнения заданий дать команду на смену, чтобы оба члена расчета получили практические навыки. Использовать ПЭВМ под управлением ОС Microsoft Windows. Проверить результаты выполнения курсантами заданий, при необходимости задать дополнительные вопросы и оценить ответы обучающихся. Обратить внимание на:

работу по настройке политики безопасности на ПЭВМ путём разрешения, запрещения доступа другим пользователям с помощью МЭ.

Лекция № 14 – Общие сведения о компьютерных вирусах.

Материал лекции должен содержать и раскрывать суть рассматриваемых учебных вопросов. В начале занятия провести контрольный опрос для контроля усвоения материала предыдущей лекции. С целью повышения наглядности на лекции целесообразно использовать: презентации, плакаты, раздаточный материал. Лектор должен разъяснить курсантам особенности изучения каждого учебного вопроса. Обратить внимание на:

История появления компьютерных вирусов и факторы, влияющие на их распространение. Понятие компьютерного вируса и основные этапы его жизненного цикла. Наиболее распространённые компьютерные вирусы и их классификация.

Лекция № 15 – Организация антивирусной защиты.

Материал лекции должен содержать и раскрывать суть рассматриваемых учебных вопросов. В начале занятия провести контрольный опрос для контроля усвоения материала предыдущей лекции. С целью повышения наглядности на лекции целесообразно использовать: презентации, плакаты, раздаточный материал. Лектор должен разъяснить курсантам особенности изучения каждого учебного вопроса. Обратить внимание на:

Уровни защиты от компьютерных вирусов. Общая характеристика сертифицированных антивирусных средств.

Практическое занятие № 8 – Работа с антивирусным комплексом Doctor Web для Windows.

В начале занятия произвести опрос курсантов по теоретическому материалу, знание которого требуется для решения задач по теме занятия. Продолжительность опроса – до 15 минут.

В случае, невозможности предоставления каждому курсанту индивидуальной ПЭВМ, работу проводить в составе утвержденных расчетов (в составе 2-х курсантов) по заданию. Выдать курсантам необходимые учебные материалы занятия и задания (каждый курсант должен получить и выполнить задание установку ОС). В ходе выполнения заданий дать команду на смену, чтобы оба члена расчета получили практические навыки. Использовать ПЭВМ под управлением ОС Microsoft Windows. Проверить результаты выполнения курсантами заданий, при необходимости задать дополнительные вопросы и оценить ответы обучающихся. Обратить внимание на:

осуществление обнаружения и удаление компьютерных вирусов (тестовых) с ПЭВМ. Научиться осуществлять обновление вирусных баз ПЭВМ с магнитных носителей.

Практическое занятие № 9 – Работа с антивирусом Касперского для Windows.

В начале занятия произвести опрос курсантов по теоретическому материалу, знание которого требуется для решения задач по теме занятия. Продолжительность опроса – до 15 минут.

В случае, невозможности предоставления каждому курсанту индивидуальной ПЭВМ, работу проводить в составе утвержденных расчетов (в составе 2-х курсантов) по заданию. Выдать курсантам необходимые учебные материалы занятия и задания (каждый курсант должен получить и выполнить задание установку ОС). В ходе выполнения заданий дать команду на смену, чтобы оба члена расчета получили практические навыки. Использовать ПЭВМ под управлением ОС Microsoft Windows. Проверить результаты выполнения курсантами заданий, при необходимости задать дополнительные вопросы и оценить ответы обучающихся. Обратить внимание на:

осуществление обнаружение и удаление компьютерных вирусов (тестовых) с ПЭВМ. Научиться осуществлять обновление вирусных баз ПЭВМ с магнитных носителей.

Практическое занятие № 10 – Работа с средством анализа защищённости XSpider.

В начале занятия произвести опрос курсантов по теоретическому материалу, знание которого требуется для решения задач по теме занятия. Продолжительность опроса – до 15 минут.

В случае, невозможности предоставления каждому курсанту индивидуальной ПЭВМ, работу проводить в составе утвержденных расчетов (в составе 2-х курсантов) по заданию. Выдать курсантам необходимые учебные материалы занятия и задания (каждый курсант должен получить и выполнить задание установку ОС). В ходе выполнения заданий дать команду на смену, чтобы оба члена расчета получили практические навыки. Использовать ПЭВМ под управлением ОС Microsoft Windows. Проверить ре-

зультаты выполнения курсантами заданий, при необходимости задать дополнительные вопросы и оценить ответы обучающихся. Обратить внимание на:

Работу со сканером безопасности «XSPIDER». Работа с CGI сканером «XSPIDER». Работа с TCP сервисами «XSPIDER». Перенаправление данных через TCP порт «XSPIDER». Работа с UDP дата граммами IP пакетами «XSPIDER». Составление отчёта о ходе выполнения предыдущих заданий.

Лекция № 16 – Общие сведения об операционной системе МСВС.

Материал лекции должен содержать и раскрывать суть рассматриваемых учебных вопросов. В начале занятия провести контрольный опрос для контроля усвоения материала предыдущей лекции. С целью повышения наглядности на лекции целесообразно использовать: презентации, плакаты, раздаточный материал. Лектор должен разъяснить курсантам особенности изучения каждого учебного вопроса. Обратить внимание на:

Общие сведения о реализации защиты ИПО в операционных системах. Назначение состав и основные возможности ОС МСВС. Основные задачи администратора системы (подключение пользователей, резервное копирование, мониторинг системы и др.).

Лекция № 17 – Система защиты от НСД ОС МСВС.

Материал лекции должен содержать и раскрывать суть рассматриваемых учебных вопросов. В начале занятия провести контрольный опрос для контроля усвоения материала предыдущей лекции. С целью повышения наглядности на лекции целесообразно использовать: презентации, плакаты, раздаточный материал. Лектор должен разъяснить курсантам особенности изучения каждого учебного вопроса. Обратить внимание на:

Состав и характеристика основных элементов «Система защиты от НСД». Контроль целостности файловой системы.

Лекция № 18 – Система защиты от НСД ОС МСВС.

Материал лекции должен содержать и раскрывать суть рассматриваемых учебных вопросов. В начале занятия провести контрольный опрос для контроля усвоения материала предыдущей лекции. С целью повышения наглядности на лекции целесообразно использовать: презентации, плакаты, раздаточный материал. Лектор должен разъяснить курсантам особенности изучения каждого учебного вопроса. Обратить внимание на:

Командный и графический интерфейс СЗИ ОС МСВС. Программы резервного копирования.

Практическое занятие № 11 – Система контроля целостности Aide операционной системы МС ВС.

В начале занятия произвести опрос курсантов по теоретическому материалу, знание которого требуется для решения задач по теме занятия. Продолжительность опроса – до 15 минут.

В случае, невозможности предоставления каждому курсанту индивидуальной ПЭВМ, работу проводить в составе утвержденных расчетов (в составе 2-х курсантов) по заданию. Выдать курсантам необходимые учебные материалы занятия и задания (каждый курсант должен получить и выполнить задание установку ОС). В ходе выполнения заданий дать команду на смену, чтобы оба члена расчета получили практические навыки. Использовать ПЭВМ под управлением ОС Microsoft Windows и гостевой ОС МСВС 3.0. Проверить результаты выполнения курсантами заданий, при необходимости задать дополнительные вопросы и оценить ответы обучающихся. Обратить внимание на:

Настройка и работа с системой контроля целостности Aide в ОС МС ВС 3.0. Создание скрипта для автоматизации запуска процесса проверки.

Практическое занятие № 12 – Архивация и восстановление данных в ОС МС ВС.

В начале занятия произвести опрос курсантов по теоретическому материалу, знание которого требуется для решения задач по теме занятия. Продолжительность опроса – до 15 минут.

В случае, невозможности предоставления каждому курсанту индивидуальной ПЭВМ, работу проводить в составе утвержденных расчетов (в составе 2-х курсантов) по заданию. Выдать курсантам необходимые учебные материалы занятия и задания (каждый курсант должен получить и выполнить задание установку ОС). В ходе выполнения заданий дать команду на смену, чтобы оба члена расчета получили практические навыки. Использовать ПЭВМ под управлением ОС Microsoft Windows и гостевой ОС МСВС 3.0. Проверить результаты выполнения курсантами заданий, при необходимости задать дополнительные вопросы и оценить ответы обучающихся. Обратить внимание на:

Установка и настройка средства управления резервным копированием КСЗИ СВАС. Немедленная и плановая архивация данных в ОС МС ВС. Восстановление данных в ОС МС ВС 3.0 с помощью средства управления резервным копированием КСЗИ СВАС.

Практическое занятие № 13 – Работа с антивирусным комплексом DrWeb для ОС МСВС 3.0.

В начале занятия произвести опрос курсантов по теоретическому материалу, знание которого требуется для решения задач по теме занятия. Продолжительность опроса – до 15 минут.

В случае, невозможности предоставления каждому курсанту индивидуальной ПЭВМ, работу проводить в составе утвержденных расчетов (в составе 2-х курсантов) по заданию. Выдать курсантам необходимые учебные материалы занятия и задания (каждый курсант должен получить и выполнить задание установку ОС). В ходе выполнения заданий дать команду на смену, чтобы оба члена расчета получили практические навыки. Использовать ПЭВМ под управлением ОС Microsoft Windows и гостевой ОС МСВС 3.0. Проверить результаты выполнения курсантами заданий, при необходимости задать дополнительные вопросы и оценить ответы обучающихся. Обратить внимание на:

Установка антивирусного комплекса DrWeb на ПЭВМ. Обновление антивирусных баз ПЭВМ с магнитных носителей.

Практическое занятие № 14 «Особенности работы с ПО РМ АБИ

В начале занятия произвести опрос курсантов по теоретическому материалу, знание которого требуется для решения задач по теме занятия. Продолжительность опроса – до 15 минут.

В случае, невозможности предоставления каждому курсанту индивидуальной ПЭВМ, работу проводить в составе утвержденных расчетов (в составе 2-х курсантов) по заданию. Выдать курсантам необходимые учебные материалы занятия и задания (каждый курсант должен получить и выполнить задание установку ОС). В ходе выполнения заданий дать команду на смену, чтобы оба члена расчета получили практические навыки. Использовать ПЭВМ под управлением ОС Microsoft Windows и гостевой ОС МСВС 3.0. Проверить результаты выполнения курсантами заданий, при необходимости задать дополнительные вопросы и оценить ответы обучающихся. Обратить внимание на:

«Систему защиты от НСД ОС МСВС 3.0». Настройка средств управления РМ АОБИ. Составление отчета о проделанной работе и его защита.

Лекция № 19 – Комплексное обеспечение информационной безопасности АС.

Материал лекции должен содержать и раскрывать суть рассматриваемых учебных вопросов. В начале занятия провести контрольный опрос для контроля усвоения материала предыдущей лекции. С целью повышения наглядности на лекции целесообразно использовать: презентации, плакаты, раздаточный материал. Лектор должен разъяснить курсантам особенности изучения каждого учебного вопроса. Обратить внимание на:

Принципы построения комплексной системы информационной безопасности объекта. Порядок разработки комплексной системы обеспечения информационной безопасности объекта. Основные этапы создания системы информационной безопасности. План мероприятий по защите служебной или коммерческой тайны. Организационные меры обеспечения защиты информации. Автоматизированный комплекс обеспечения безопасности.

Практическое занятие № 15 – Проектирование системы комплексного обеспечения информационной безопасности АС.

В начале занятия произвести опрос курсантов по теоретическому материалу, знание которого требуется для решения задач по теме занятия. Продолжительность опроса – до 15 минут.

В случае, невозможности предоставления каждому курсанту индивидуальной ПЭВМ, работу проводить в составе утвержденных расчетов (в составе 2-х курсантов) по заданию. Выдать курсантам необходимые учебные материалы занятия и задания (каждый курсант должен получить и выполнить задание установку ОС). В ходе выполнения заданий дать команду на смену, чтобы оба члена расчета получили практические навыки. Использовать ПЭВМ под управлением ОС Microsoft Windows и гостевой ОС МСВС 3.0. Проверить результаты выполнения курсантами заданий, при необходимости задать дополнительные вопросы и оценить ответы обучающихся. Обратить внимание на:

Разработка плана используемых ресурсов и средств для обеспечения информационной безопасности АС. Настройка используемых программных средств обеспечения информационной безопасности АС. Составление отчёта о проделанной работе.

Практическое занятие № 16 «Настройка межсетевого экрана в МСВС 3.0».

В начале занятия произвести опрос курсантов по теоретическому материалу, знание которого требуется для решения задач по теме занятия. Продолжительность опроса – до 15 минут.

В случае, невозможности предоставления каждому курсанту индивидуальной ПЭВМ, работу проводить в составе утвержденных расчетов (в составе 2-х курсантов) по заданию. Выдать курсантам необходимые учебные материалы занятия и задания (каждый курсант должен получить и выполнить задание установку ОС). В ходе выполнения заданий дать команду на смену, чтобы оба члена расчета получили практические навыки. Использовать ПЭВМ под управлением ОС Microsoft Windows и гостевой ОС МСВС 3.0. Проверить результаты выполнения курсантами заданий, при необходимости задать дополнительные вопросы и оценить ответы обучающихся. Обратить внимание на:

Правила фильтрации пакетов межсетевым экраном. Настройка межсетевого экрана для МСВС 3.0.

Практическое занятие № 17 – Инструментальные средства обеспечения сертификационных испытаний программного обеспечения на отсутствие не декларированных возможностей.

В начале занятия произвести опрос курсантов по теоретическому материалу, знание которого требуется для решения задач по теме занятия. Продолжительность опроса – до 15 минут.

В случае, невозможности предоставления каждому курсанту индивидуальной ПЭВМ, работу проводить в составе утвержденных расчетов (в составе 2-х курсантов) по заданию. Выдать курсантам необходимые учебные материалы занятия и задания (каждый курсант должен получить и выполнить задание установку ОС). В ходе выполнения заданий дать команду на смену, чтобы оба члена расчета получили практические навыки. Использовать ПЭВМ под управлением ОС Microsoft Windows. Проверить результаты выполнения курсантами заданий, при необходимости задать дополнительные вопросы и оценить ответы обучающихся. Обратить внимание на:

Установка и настройка дизассемблера IDA Pro. Дизассемблирование программных средств, имеющих (не имеющих) программные модули защиты с помощью IDA Pro.

Практическое занятие № 18 – Защита разработанной комплексной системы информационной безопасности АС в зависимости от задания преподавателя.

В начале занятия произвести опрос курсантов по теоретическому материалу, знание которого требуется для решения задач по теме занятия. Продолжительность опроса – до 15 минут.

В случае, невозможности предоставления каждому курсанту индивидуальной ПЭВМ, работу проводить в составе утвержденных расчетов (в составе 2-х курсантов) по заданию. Выдать курсантам необходимые учебные материалы занятия и задания (каждый курсант должен получить и выполнить задание установку ОС). В ходе выполнения заданий дать команду на смену, чтобы оба члена расчета получили практические навыки. Использовать ПЭВМ под управлением ОС Microsoft Windows. Проверить результаты выполнения курсантами заданий, при необходимости задать дополнительные вопросы и оценить ответы обучающихся.

Далее необходимо, чтобы каждый расчет защитил отчет по разработанной системе комплексного обеспечения информационной безопасности в виде дискуссии «нападение-защита». Подведение итогов, выставление оценок.

Лекция 20 – Заключение.

В заключительной лекции сделать краткий обзор изученного материала. Дать рекомендации по самостоятельному изучению материала и совершенствованию знаний в области защиты информации. Озвучить проблемы обеспечения информационной безопасности отечественных информационных систем. Кратко перечислить перспективы и тенденции развития защиты информации.

Основными формами и методами формирования у выпускников навыков и умений являются тренировка в администрировании сертифицированных средств защиты информации, применении на практике систем программирования для разработки специального программного обеспечения решения военно-прикладных задач в процессе практических занятий и курсового проектирования.

Промежуточная аттестация по дисциплине в седьмом семестре – защита курсовой работы, в восьмом семестре – экзамен. Примерная тематика курсовых работ, перечень вопросов и практических заданий по дисциплине представлены в рабочей програм-

ме. Экзаменационные билеты составлять на основе фонда контрольных заданий. При выставлении итоговой оценки учитывать результаты выполнения курсовой работы.

Тематический план рассмотрен на заседании кафедры, протокол «__» _____ 202_ г., № ___

Доцент 27 кафедры

подполковник_____ С.Краснов

УТВЕРЖДАЮ
Начальник __ кафедры
полковник
С.Войцеховский
___ _____ 202___г.

ИЗМЕНЕНИЯ, ВНЕСЕННЫЕ В ТЕМАТИЧЕСКИЙ ПЛАН ПОСЛЕ ЕГО КОРРЕКТИРОВКИ

на _____ учебный год

I. Произведено перераспределение учебного времени по видам учебных занятий

Семестры	Трудоемкость дисциплины (модуля), зач.ед/ час.	Контактная работа обучающихся с преподавателем	В том числе												Самостоятельная работа обучающихся	Отчетность за изучение дисциплины (модуля)
			лекции	семинары	лабораторные работы	практические занятия	групповые упражнения	групповые занятия	тактические (тактико-специальные) занятия и учения	кшу, военные (военно-специальные) игры	контрольные работы (занятия)	курсовые работы (проекты, задачи)	другие виды учебных занятий	Экзамены, зачеты		

II. Изменения, внесенные в план изучения дисциплины по видам учебных занятий

№ п/п	Виды учебных занятий	Кол-во часов	Наименование разделов и тем, учебные вопросы занятия	Материально-техническое и информационно-методическое обеспечение занятия	Задания на самостоятельную работу	
					Задание и литература (номер учебника или уч. пособия и номера страниц)	Время (в часах)
1	2	3	4	5	6	7

III. Методические указания, литература и другие указания

IV. Основание для внесения изменений в тематический план
(директива, рапорт или другие документы)

Изменения, внесенные в тематический план, рассмотрены и одобрены на заседании кафедры __ _____ 202__ г., протокол № _____

_____ ___ кафедры

_____
(инициал имени и фамилия)

«____»_____202__ г.

В настоящем журнале прошнуровано и скреплено печатью _____ листов.

Начальник 27 кафедры

полковник _____ С. Войцеховский
(воинское звание) подпись (инициал имени и фамилия)