МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Факультет информатики и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Программно-аппаратные средства защиты информации

Кафедра **Информатики и информационных технологий**
факультета **Информатики и информационных технологий**

Образовательная программа
10.03.01 Информационная безопасность

Профиль подготовки: Безопасность компьютерных систем

Уровень высшего образования: бакалавриат

Форма обучения
Очная

Статус дисциплины: базовая

Махачкала, 2018

Рабочая программа дисциплины Программно-аппаратные средства защиты информации составлена в 2018 году в соответствии требованиями ФГОС ВО по направлению подготовки 10.03.01 Информационная безопасность (уровень бакалавриата) от « 01» декабря 2016 г. № 1515

Разработчик: каф. информатики и информационных технологий Гаджиев А.М., кандидат физ. – мат. наук, доцент.

Рабочая программа дисциплины одобрена:
на заседании информатики и информационных технологий

от « 02 » июля 2018г. протокол №12

Зав. кафедрой _____ Ахмедов С.А.
(подпись)

На заседании Методической комиссии Информатики и информационных технологий факультета от

« 03 » июля 2018г., протокол № 10

Председатель _____ Камилов К.Б.

(подпись)

Рабочая программа дисциплины согласована с учебно-методическим управлением

« 18 » 08 2018 г. _____

(подпись)

Аннотация рабочей программы дисциплины

Дисциплина Программно-аппаратные средства защиты информации входит в базовую часть образовательной программы бакалавриата по направлению 10.03.01 Информационная безопасность.

Дисциплина реализуется на факультете Информатики и информационных технологий кафедрой Информатики и информационных технологий.

Содержание дисциплины: Программно-аппаратные средства обеспечения ЗИ. Методы и средства защиты программного обеспечения. Построение изолированной программной среды. Удаленные сетевые атаки. Технологии межсетевого экранирования. Системы обнаружения атак и вторжений. Виртуальные частные сети. Стандарты информационной безопасности.

Дисциплина нацелена на формирование следующих компетенций выпускника: общекультурных - ОК-5, общепрофессиональных – ОПК-3, ОПК-7, профессиональных ПК-4, ПК-5, ПК-6.

Рабочая программа дисциплины предусматривает проведение следующих видов контроля успеваемости в форме контрольных работ и промежуточный контроль в форме экзамена.

Преподавание дисциплины предусматривает проведение следующих видов учебных занятий: лекции, практические занятия, лабораторные занятия, самостоятельная работа.

Объем дисциплины 4 зачетных единиц, в том числе в академических часах по видам учебных занятий.

Семестр	Учебные занятия								Форма промежуточной аттестации (зачет, дифференцированный зачет, экзамен
	в том числе:								
	всего	Контактная работа обучающихся с преподавателем						СРС, в том числе экзамен	
		всего	из них						
			Лекции	Лабораторные занятия	Практические занятия	КСР	контроль		
7	144	72	36	18	18		36	36	экзамен

1. Цели освоения дисциплины

Формирование у студентов знаний по основам защиты информации в компьютерных системах при помощи программно-аппаратных средств, а также навыков и умения в применении знаний для конкретных условий.

2. Место дисциплины в структуре ОПОП бакалавриата

Дисциплина Программно-аппаратные средства защиты информации входит в профессиональный цикл, базовую часть образовательной программы бакалавриата по направлению (специальности) 10.03.01 Информационная безопасность.

Для эффективного освоения дисциплины требуются знания по криптографическим методам защиты информации, технической защите информации, основам информационной безопасности.

3. Компетенции обучающегося, формируемые в результате освоения дисциплины (перечень планируемых результатов обучения).

Процесс изучения дисциплины направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВПО по данному направлению:

Код компетенции из ФГОС ВО	Наименование компетенции из ФГОС ВО	Планируемые результаты обучения
ОК-5	способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией у выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	*Знает:* Методы анализа информации. *Умеет:* Находить актуальную информацию и ставить цели. *Владеет:* Средствами поиска и анализа информации.
ОПК-3	способностью применять положения электротехники, электроники и схемотехники для решения профессиональных задач	*Знает:* Способы обеспечения ИБ. *Умеет:* применять меры по обеспечению ИБ. *Владеет:* современными навыками по настройке и обслуживанию средств
ОПК-7	способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и	*Знает:* теоретические основы анализа данных *Умеет:* собирать данные и проводить их анализ с использованием программного обеспечения *Владеет:* навыками сбора и анализа данных полученных

	содержания информационных процессов и особенностей функционирования объекта защиты	
ПК-4	способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	*Знает:* теоретические основы анализа и обеспечения информационной безопасности данных *Умеет:* применять комплексный подход к обеспечению информационной безопасности *Владеет:* навыками сбора и анализа данных, способностью участвовать в работах по реализации политики информационной безопасности
ПК-5	способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	*Знает:* теоретические положения и нормативы по организации и сопровождении аттестации объекта информатизации по требованиям безопасности *Умеет:* осуществлять контроль и аттестацию объекта информатизации по требованиям безопасности информации *Владеет:* способами и методами безопасности по организации и сопровождении аттестации объекта информатизации
ПК-6	способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	*Знает:* нормативные положения и регламент при проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации *Умеет:* применять теоретические знания и практические навыки при проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации *Владеет:* навыками работы по обеспечению контрольных проверок работоспособности и эффективности программных, программно-аппаратных и технических средств защиты информации

4. Объем, структура и содержание дисциплины.

4.1. Объем дисциплины составляет 4 зачетных единиц, 72 академических часа.

4.2. Структура дисциплины.

№ п/п	Разделы и темы дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)				Самостоятельная работа	Формы текущего контроля успеваемости *(по неделям семестра)* Форма промежуточной аттестации *(по семестрам)*
				Лекции	Практические занятия	Лабораторные занятия	Контроль самост. раб.		
	Модуль 1. ***Введение в программно-аппаратную защиту***								
1	Проблемы информационной безопасности	7	1	2	2		2		устный и письменный опросы
2	Стандарты информационной безопасности	7	2	2	2		2		устный и письменный опросы
3	Системы контроля и управления доступом	7	3	2		2	2		Устный опрос. Защита л.р.
4	Идентификация пользователей КС - объектов доступа к данным	7	4	2		2	2		устный и письменный опросы
5	Средства и методы ограничения доступа к файлам	7	5	2		2	2		устный и письменный опросы
6	Видеонаблюдение	7	6	2	2		2		устный и письменный опросы
	Итого по модулю 1:			12	6	6	12		36
	Модуль 2. ***Обеспечение защиты на корпоративном уровне***								
1	Идентификация, аутентификация и управление доступом	7	7	2		2	2		устный и письменный опросы
2	Защита программ от несанкционированного копирования	7	8	2		2	2		Устный опрос. Защита л.р.
3	Принципы многоуровневой защиты корпоративной информации	7	9	2	2		2		устный и письменный опросы
4	Обеспечение безопасности операционных систем	7	10	2	2		2		устный и письменный опросы
5	Протоколы защиты каналов	7	11	2		2	2		устный и письменный опросы
6	Обзор	7	12	2	2		2		устный и письменный

	современных систем управления безопасностью								опросы
	Итого по модулю 2:			12	6	6	12		36
	Модуль 3. ***Управление безопасностью в глобальной сети***								
1	Технологии межсетевого экранирования	7	13	2		2	2		устный и письменный опросы
2	Технологии виртуальной защиты сетей VPN	7	14	2		2	2		Устный опрос. Защита л.р.
3	Защита удаленного доступа.	7	15	2		2	2		устный и письменный опросы
4	Технологии обнаружения и предотвращения вторжений	7	16	2	2		2		устный и письменный опросы
5	Технологии защиты от вредоносных программ и спама	7	17	2	2		2		устный и письменный опросы
6	Управление средствами обеспечения информационной безопасности	7	18	2	2		2		устный и письменный опросы
	Итого по модулю 3:			12	6	6	12		36
	Модуль 4. ***Подготовка к экзамену***								
	Итого по модулю 4:							36	36
	ИТОГО:			36	18	18	36	36	144

4.3. Содержание дисциплины, структурированное по темам (разделам).

4.3.1. Содержание лекционных занятий по дисциплине.

Модуль 1. Введение в программно-аппаратную защиту

Тема 1. Политика информационной безопасности.

Содержание темы. Определяются базовые понятия политики безопасности и описываются основные виды политик и процедуры безопасности в корпоративных информационных системах.

Тема 2. Стандарты информационной безопасности.

Содержание темы. Даются краткие описания популярных стандартов информационной безопасности. Описываются отечественные стандарты безопасности информационных технологий.

Тема 3. Системы контроля и управления доступом.

Содержание темы. Рассматриваются принципы организации систему управления и контроля доступом, основные проблемы, преимущества и недостатки разных методов идентификации.

Тема 4. Идентификация пользователей КС - объектов доступа к данным.

Содержание темы. Понятие идентификации пользователя Задача идентификации пользователя. Понятие протокола идентификации. Локальная и удаленная идентификация.

Тема 5. Средства и методы ограничения доступа к файлам.

Содержание темы. Доступ к данным со стороны процесса.

Понятие доступа к данным со стороны процесса: отличия от доступа со стороны пользователя. Понятие и примеры скрытого доступа. Надежность систем ограничения доступа.

Особенности защиты данных от изменения.

Защита массивов информации от изменения (имитозащита). Криптографическая постановка защиты от изменения данных.

Подходы к решению задачи защиты данных от изменения. Подход на основе формирования имитоприставки (MAC), способы построения MAC. Подход на основе формирования хэш-функции, требования к построению и способы реализации. Формирование электронной цифровой подписи (ЭЦП). Особенности защиты ЭД и исполняемых файлов. Проблема самоконтроля исполняемых модулей.

Тема 6. Видеонаблюдение.

Содержание темы. Анализируются основные задачи и проблемы видеонаблюдения.

Модуль 2. Обеспечение защиты на корпоративном уровне

Тема 7**.** Идентификация, аутентификация и управление доступом.

Содержание темы Рассматриваются вопросы идентификации, аутентификации и авторизации пользователя. Описываются методы аутентификации.

Тема 8. Защита программ от несанкционированного копирования.

Содержание темы. Рассматриваются вопросы несанкционированного копирования программ. Несанкционированное копирование программ как тип НСД. Юридические аспекты несанкционированного копирования программ. Общее понятие зашиты от копирования. Разновидности задач защиты от копирования.

Тема 9. Принципы многоуровневой защиты корпоративной информации.

Содержание темы. Описываются стратегии многоуровневой защиты КИС. Рассматривается безопасность «облачных» вычислений.

Тема 10. Обеспечение безопасности операционных систем.

Содержание темы. Рассматриваются средства обеспечения безопасности ОС UNIX и Windows 7.

Тема 11. Протоколы защиты каналов.

Содержание темы. Описывается архитектура протоколов IPSec, протокол аутентификации AH, протокол формирования защищенного пакета ESP, протокол управления криптоключами ПСЕ. Приводятся сведения об алгоритмах аутентификации и шифрования, применяемых в стеке протоколов IPSec.

Тема 12. Обзор современных систем управления безопасностью.

Содержание темы. Обзор современных систем управления информационной безопасностью.

Модуль 3. Управление безопасностью в глобальной сети

Тема 1**3.** Технологии межсетевого экранирования.

Содержание темы Рассматриваются функции межсетевых экранов. Описываются схемы сетевой защиты на базе межсетевых экранов.

Тема 14. Технологии виртуальной защиты сетей VPN.

Содержание темы. Рассматриваются защищенные виртуальные сети VPN (Virtual Private Network). Поясняется главное свойство VPN - тунелирование. Анализируются варианты построения виртуальных защищенных каналов.

Тема 15. Защита удаленного доступа.

Содержание темы. Рассматривается организация защищенного удаленного доступа, анализируются протоколы аутентификации системы централизованного контроля удаленного доступа.

Тема 16. Технологии обнаружения и предотвращения вторжений.

Содержание темы. Рассматриваются проблемы обнаружения и предотвращения вторжений.

Тема 17. Технологии защиты от вредоносных программ и спама.

Содержание темы. Технологии защиты от внешних программ и спама. Приводится классификация вредоносных программ.

Тема 18. Управление средствами обеспечения информационной безопасности.

Содержание темы. Методы управления средствами защиты корпоративной информации. Формулируются задачи управления системной информационной безопасностью масштаба предприятия.

4.3.2. Содержание лабораторно-практических занятий по дисциплине.

Модуль 1. Введение в программно-аппаратную защиту

Тема 1. Политика информационной безопасности.

Содержание темы. Определяются базовые понятия политики безопасности и описываются основные виды политик и процедуры безопасности в корпоративных информационных системах.

Тема 2. Стандарты информационной безопасности.

Содержание темы. Рассматриваются основные международные стандарты информационной безопасности.

Тема 3. Системы контроля и управления доступом.

Содержание темы. Рассматриваются принципы организации систему управления и контроля доступом, основные проблемы, преимущества и недостатки разных методов идентификации.

Тема 4. Идентификация пользователей КС - объектов доступа к данным.

Содержание темы. Идентифицирующая информация. Понятие идентифицирующей информации. Способы хранения идентифицирующей информации. Связь с ключевыми системами.

Тема 5. Средства и методы ограничения доступа к файлам.

Содержание темы. Основные подходы к защите данных от НСД.

Шифрование. Контроль доступа. Разграничения доступа. Файл как объект доступа. Оценка надежности систем ограничения доступа - сведение к задаче оценки стойкости.

Организация доступа к файлам.

Иерархический доступ к файлам. Понятие атрибутов доступа. Организация доступа к файлам в различных ОС. Защита сетевого файлового ресурса на примерах организации доступа в ОС UNIX, Novell NetWare и т. д.

Фиксация доступа к файлам.

Способы фиксации фактов доступа. Журналы доступа. Критерии информативности журналов доступа. Выявление следов несанкционированного доступа к файлам, метод инициированного НСД.

Тема 6. Видеонаблюдение.

Содержание темы. Рассматриваются виды камер и регистраторов, и их отличия. Уделяется внимание параметрам, определяющим качество изображения, а также оптическим компонентам системы видеонаблюдения.

Модуль 2. Обеспечение защиты на корпоративном уровне

Тема 7**.** Идентификация, аутентификация и управление доступом.

Содержание темы Использующие многоразовые и одноразовые пароли, протоколы строгой аутентификации, смарт карты и USB-токены, биометрическую аутентификацию пользователей, управление доступом по схеме однократного входа Single Sign-On.

Тема 8. Защита программ от несанкционированного копирования.

Содержание темы. Анализируются методов защиты от копирования Привязка ПО к аппаратному окружению и физическим носителям как единственное средство защиты от копирования ПО. Привязка программ к гибким магнитным дискам (ГМД). Структура данных на ГМД. Управление контроллером ГМД. Способы создания некопируемых меток. Точное измерение характеристик форматирования дорожки. Технология "слабых битов". Физические метки и технология работы с ними. Привязка программ к жестким магнитным дискам (ЖМД). Особенности привязки к ЖМД. Виды меток на ЖМД. Привязка к прочим компонентам штатного оборудования ПЭВМ. Привязка к внешним (добавляемым) элементам ПЭВМ. Привязка к портовым ключам. Использование дополнительных плат расширения. Методы "водяных знаков" и методы "отпечатков пальцев".

Тема 9. Принципы многоуровневой защиты корпоративной информации.

Содержание темы. Рассматриваются принципы комплексной многоуровневой защиты информации в корпоративных системах. Анализируются традиционные структуры корпоративных информационных систем и инфраструктура «облачных» вычислений.

Тема 10. Обеспечение безопасности операционных систем.

Содержание темы. Анализируются угрозы безопасности в операционных системах, вводится понятие защищенной ОС.

Тема 11. Протоколы защиты каналов.

Содержание темы. Рассматриваются проблемы построения защищенных виртуальных каналов на канальном, сетевом и сеансовом уровнях OSI. Рассматриваются особенности применения протоколов на канальном уровне PPTP, L2F и L2TP.

Тема 12. Обзор современных систем управления безопасностью.

Содержание темы. Рассматриваются продукты компании ЭЛВИС+, Cisco Systems, IBM, Check Point для управления средствами управления безопасности.

Модуль 3. Управление безопасностью в глобальной сети

Тема 1**3.** Технологии межсетевого экранирования.

Содержание темы Рассматривается применение персональных и распределенных сетевых экранов.

Тема 14. Технологии виртуальной защиты сетей VPN.

Содержание темы. Рассматриваются варианты архитектуры сети VPN и приводятся основные виды технической реализации VPN.

Тема 15. Защита удаленного доступа.

Содержание темы. Рассматривается организация защищенного удаленного доступа, анализируются протоколы аутентификации системы централизованного контроля удаленного доступа.

Тема 16. Технологии обнаружения и предотвращения вторжений.

Содержание темы. Рассматриваются методы обнаружения и предотвращения вторжений в корпоративные системы, а также защита от распределенных атак.

Тема 17. Технологии защиты от вредоносных программ и спама.

Содержание темы. Рассматривается сигнатурный анализ и проактивные методы обнаружения вирусов и других вредоносных программ.

Тема 18. Управление средствами обеспечения информационной безопасности.

Содержание темы. Анализируются варианты архитектуры управления средствами безопасности. Особое внимание уделяется перспективной архитектуре централизованного управления безопасностью на базе глобальной и локальной политик безопасности.

5. Образовательные технологии

Рекомендуемые образовательные технологии: лекции, лабораторные занятия, самостоятельная работа студентов.

В соответствии с требованиями ФГОС ВО по направлению подготовки реализация компетентностного подхода предусматривает широкое использование в учебном процессе активных и интерактивных форм проведения занятий (компьютерных симуляций, разбор конкретных ситуаций) в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.

Удельный вес занятий, проводимых в интерактивных формах, определяется главной целью (миссией) программы, особенностью контингента обучающихся и содержанием конкретных дисциплин, и в целом

в учебном процессе они должны составлять не менее 30% аудиторных занятий (определяется требованиями ФГОС с учетом специфики ОПОП). Занятия лекционного типа для соответствующих групп студентов не могут составлять более 60% аудиторных занятий (определяется соответствующим ФГОС)).

6. Учебно-методическое обеспечение самостоятельной работы студентов.

Для осуществления самостоятельной работы студентов используются учебники, рекомендованные в литературном списке, методические пособия, которые существуют как в печатном варианте, так и в электронном варианте, в том числе содержащиеся в сети на сайте университета

Форма контроля и критерий оценок

В соответствии с учебным планом предусмотрен экзамен в 7 семестре.

Формы контроля: текущий контроль, промежуточный контроль по модулю, итоговый контроль по дисциплине предполагают следующее распределение баллов.

Текущий контроль

Посещаемость занятий 5 баллов

Выполнение 1 лабораторной работы 5 баллов

Промежуточный контроль

По завершении модуля проводить устный опрос 60 баллов

7. Фонд оценочных средств для проведения текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины.

7.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы.

Перечень компетенций с указанием этапов их формирования приведен в описании образовательной программы.

Код компетенции из ФГОС ВО	**Наименование компетенции из ФГОС ВО**	**Планируемые результаты обучения**	**Процедура освоения**
ОК-5	способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией у выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества	*Знает:* Методы анализа информации. *Умеет:* Находить актуальную информацию и ставить цели. *Владеет:* Средствами поиска и анализа информации.	Устный опрос, письменный опрос

	и государства, соблюдать нормы профессиональной этики		
ОПК-3	способностью применять положения электротехники, электроники и схемотехники для решения профессиональных задач	*Знает:* Способы обеспечения ИБ. *Умеет:* применять меры по обеспечению ИБ. *Владеет:* современными навыками по настройке и обслуживанию средств	Устный опрос, письменный опрос
ОПК-7	способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	*Знает:* теоретические основы анализа данных *Умеет:* собирать данные и проводить их анализ с использованием программного обеспечения *Владеет:* навыками сбора и анализа данных полученных	Устный опрос, письменный опрос
ПК-4	способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	*Знает:* теоретические основы анализа и обеспечения информационной безопасности данных *Умеет:* применять комплексный подход к обеспечению информационной безопасности *Владеет:* навыками сбора и анализа данных, способностью участвовать в работах по реализации политики информационной безопасности	Устный опрос, письменный опрос, сдача лабораторных работ
ПК-5	способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	*Знает:* теоретические положения и нормативы по организации и сопровождении аттестации объекта информатизации по требованиям безопасности *Умеет:* осуществлять контроль и аттестацию объекта информатизации по требованиям безопасности информации	Устный опрос, письменный опрос, сдача лабораторных работ

		Владеет: способами и методами безопасности по организации и сопровождении аттестации объекта информатизации	
ПК-6	способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	*Знает:* нормативные положения и регламент при проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации *Умеет:* применять теоретические знания и практические навыки при проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации *Владеет:* навыками работы по обеспечению контрольных проверок работоспособности и эффективности программных, программно-аппаратных и технических средств защиты информации	Устный опрос, письменный опрос, сдача лабораторных работ

7.2. Типовые контрольные задания

Примеры вопросов для самоконтроля.

1. Под угрозой безопасности информации в компьютерной системе (КС) понимают:
2. Уязвимость информации — это: _____
3. Атакой на КС называют: _____
4. Искусственные угрозы исходя из их мотивов разделяются на:
5. непреднамеренным угрозам относятся: _____
6. К умышленным угрозам относятся: _____
7. Косвенными каналами утечки называют:_____
8. К косвенным каналам утечки информации относятся: ____
9. Непосредственными каналами утечки называют: _____
10. К непосредственным каналам утески информации относятся:
11. Избирательная политика безопасности подразумевает, что:
12. Полномочная политика безопасности подразумевает, что:
13. Достоверная вычислительная база - это:_____
14. Достоверная вычислительная база выполняет задачи: _____
15. Уязвимость информации — это: _____
16. Идентификация объекта - это: _____
17. Параллельная схема идентификации позволяет увеличить:
18. Какие существуют формы представления объектов,

аутентифицирующих пользователя:

19. Внешняя и внутренняя формы представления аутентифицирующего объекта должны быть:
20. Внешние объекты могут быть технически реализованы на различных носителях информации?
21. Для чего были разработаны протоколы идентификации с нулевой передачей знаний:
22. Механизм запроса-ответа используется для: _____
23. Кто разработал алгоритм идентификации с нулевой передачей знания:
24. Схему идентификации с нулевой передачей знаний предложили:
25. Для чего создается система разграничения доступа к информации:
26. Сбои, отказы технических и программных средств могут быть использованы для НСД?
27. Правильность функционирования ядра безопасности доказывается путем:
28. Мандатное управление позволяет упростить процесс регулирования доступа?
29. Матричное управление доступом предполагает использование:
30. Основной проблемой создания высокоэффективной защиты от НСД является:
31. Аппаратно-программные средства криптографической защиты информации выполняют функции:
32. Надежность защиты информации в компьютерной системе определяется:
33. Использование аппаратных средств снимает проблему:_____
34. Криптографические функции плат КРИПТОН образующие ядро системы безопасности реализуются
35. К частично контролируемым компьютерным системам можно отнести современные КС, использующие:
36. Безопасность в частично контролируемым компьютерных системах может быть обеспечена:
37. К основным компонентам сети относятся: _____
38. В качестве ключевых носителей устройств криптографической защиты
39. данных серии КРИПТОН используются: _____
40. Средства серии КРИПТОН независимо от операционной среды
41. обеспечивают: _____
42. В системе Secret Disk используется: _____
43. В чем заключается особенность системы Secret Disk:_____
44. Мастер-ключ в Устройствах криптографической защиты данных серии
45. КРИПТОН загружается: _____
46. Криптографических функций в устройствах криптографической защиты
47. данных серии КРИПТОН выполняются: _____
48. Абонентские места, персональные компьютеры или терминалы клиента являются основными компонентами сети?

49. Возможные каналы утечки информации по классификации разделяют:
50. К группе каналов утечки информации в которой основным средством
51. является человек, относятся следующие утечки: _____
52. К группе каналов утечки информации в которой основным средством
53. является аппаратура, относятся следующие утечки: _____
54. К группе каналов утечки информации в которой основным средством
55. является программа, относятся следующие утечки: _____
56. К средствам активной защиты относятся: _____
57. К средствам пассивной защиты относятся: _____
58. К средствам собственной защиты относятся:_____
59. Может ли информативный сигнал в сети электропитания быть каналом утечки информации?
60. Мероприятия по инженерно-технической защите информации от утечки по электромагнитному каналу подразделяются на:
61. Технические мероприятия направлены: _____
62. Организационными мероприятиями предусматривается:_____
63. Активные способы защиты информации при ее утечке через сеть
64. электропитания направленные на:_____
65. Пассивные способы защиты информации при ее утечке через сеть
66. электропитания направленные на:_____
67. Для минимизации паразитных связей внутри ПЭВМ используются:
68. Под системой защиты от несанкционированного использования и
69. копирования понимается
70. Под надежностью системы защиты от несанкционированного
71. копирования понимается:
72. Методы, затрудняющие считывание скопированной информации
73. основываются на: _
74. Для защиты от несанкционированного использования программ могут применяться электронные ключи?
75. Мероприятия по инженерно-технической защите информации от утечки
76. по электромагнитному каналу подразделяются на: _____
77. Любая криптографическая система основана на использовании:
78. В симметричной криптосистеме отправитель и получатель сообщения
79. используют: _
80. Асимметричная криптосистема предполагает использование:
81. Под ключевой информацией понимают: _____
82. В каких режимах может выполняться изучение логики работы

Перечень вопросов к экзамену (7 семестр).

1. Основные функции подсистемы защиты ОС.
2. Базовая политика безопасности.
3. Специализированные политики безопасности.
4. Избирательная и полномочная политика безопасности.

5. Процедуры безопасности.
6. Разработка политики безопасной организации.
7. Управление информационными потоками.
8. Достоверная вычислительная база.
9. Механизмы защиты ДВБ.
10. Принципы реализации политики безопасности.
11. Основные критерии оценки безопасности систем.
12. Роли и ответственность в безопасности сети.
13. Идентификация и аутентификация пользователя.
14. Аутентификация на основе многоразовых паролей.
15. Аутентификация на основе одноразовых паролей.
16. Строгая аутентификация. Основные понятия.
17. Типовые схемы идентификации и аутентификации пользователя.
18. Взаимная проверка подлинности пользователей.
19. Упрощенная схема идентификации с нулевой передачей знаний.
20. Параллельная схема идентификации с нулевой передачей знаний.
21. Схема идентификации Гиллоу-Куискуотера.
22. Защита информации в КС от несанкционированного доступа.
23. Управление доступом (Система разграничения доступа к информации в КС).
24. Состав системы разграничения доступа (Система разграничения доступа к информации в КС).
25. Концепция построения систем разграничения доступа.
26. Организация доступа к ресурсам КС.
27. Обеспечение целостности и доступности информации в КС.
28. Основные понятия криптографической защиты информации.
29. Симметричные криптосистемы шифрования.
30. Асимметричные криптосистемы шифрования.
31. Функции хеширования.
32. Электронная цифровая подпись.
33. Управление криптоключами.
34. Корпоративная информационная системы.
35. Архитектура «облачных сервисов».
36. Подсистемы информационной безопасности традиционных КИС.
37. Средства защиты в виртуальных средах.
38. Обеспечение безопасности «облачных» сред на базе пакета Trend Micro Deep Security.
39. Защита на канальном уровне. Протокол PPTP.
40. Защита на канальном уровне. Протокол L2TP.
41. Защита на сетевом уровне. Архитектура средств безопасности IPSec.
42. Защита передаваемых данных с помощью протоколов AH и ESP.
43. Протокол управления криптоключами IKE.
44. База данных SAD и SPD.
45. Особенности реализации средств IPSec и их преимущества.

46. Протоколы SSL и TLS.
47. Протокол SOCKS.
48. Особенности безопасности беспроводных сетей.
49. Функции межсетевых экранов.
50. Фильтрация трафика (технологии межсетевого экранирования).
51. Выполнение функций посредничества.
52. Межсетевые экраны.
53. Классификация сети VPN и Средства обеспечения безопасности VPN.
54. Функционирование системы управления доступом.
55. Аутентификации удаленных пользователей на основе одноразовых паролей OTP.
56. Протоколы аутентификации удаленных пользователей. Протокол PAP.
57. Протоколы аутентификации удаленных пользователей. Протокол CHAP.
58. Протоколы аутентификации удаленных пользователей. Протокол EAP.
59. Протоколы аутентификации удаленных пользователей. Протокол S/Key.
60. Протоколы аутентификации удаленных пользователей. Протокол Kerberos.

Методические материалы определяющие процедуру оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

Общий результат выводится как интегральная оценка, складывающая из текущего контроля - 50% и промежуточного контроля - 50%.

Текущий контроль по дисциплине включает:

- посещение занятий - 3 баллов,
- участие на практических занятиях - 3 баллов,
- выполнение лабораторных заданий - 10 баллов,
- выполнение домашних (аудиторных) контрольных работ - 5 баллов. Промежуточный контроль по дисциплине включает:
- устный опрос - 3 баллов,
- письменная контрольная работа - 5 баллов,
- тестирование - 10 баллов.

8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

а) основная литература:

1. Платонов, Владимир Владимирович. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей : учеб. пособие для студентов вузов, обуч. по специальности 090102 "Компьютерная безопасность", 090105 "Комплексное обеспечение информ.

безопасности автоматизированных систем" / Платонов, Владимир Владимирович. - М. : Академия, 2006. - 238,[1] с. - (Высшее профессиональное образование. Информационная безопасность). - Допущено УМО. - ISBN 5-7695-2706-4 : 170-50. Местонахождение: Научная библиотека ДГУ URL:

2. Шаньгин, Владимир Фёдорович. Информационная безопасность компьютерных систем и сетей : учеб. пособие для студентов учреждений сред. проф. образования, обуч. по группе специальностей 2200 "Информатика и вычислительная техника" / Шаньгин, Владимир Фёдорович. - М. : ФОРУМ: ИНФРА-М, 2008. - 415 с. - (Профессиональное образование). - Рекомендовано МО РФ. - 194-92. Местонахождение: Научная библиотека ДГУ URL

3. Шаньгин, В.Ф. Защита компьютерной информации. Эффективные методы и средства / В. Ф. Шаньгин ; Шаньгин В. Ф. - М. : ДМК Пресс, 2010. - 544. - ISBN 978-5-94074-518-1. Местонахождение: Biblioclub URL: http://www.biblioclub.ru/book/86475/

4. Завгородний, Виктор Иванович. Комплексная защита информации в компьютерных системах : Учеб. пособие для вузов / Завгородний, Виктор Иванович. - М. : Логос, 2001. - 263 с. - ISBN 5-94010-088-0 : 114-62. Местонахождение: Научная библиотека ДГУ URL:

5. Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных: Учеб. пособие для вузов / П.Ю.Белкин, О.О.Михальский, А.С.Першаков, Д.И.Правиков и др. - М. : Радио и связь, 2000. - 168 с. : ил. - ISBN 5-256-01533-8 : 0-0. Местонахождение: Научная библиотека ДГУ URL:

б) дополнительная литература:

1. Расторгуев, Сергей Павлович. Основы информационной безопасности : учеб. пособие для студентов вузов, обуч. по специальности "Компьютер. безопасность", "Комплекс. обеспечение информ. безопасности автоматизир. систем" и "Информ. безопасность телеком. систем" / Расторгуев, Сергей Павлович. - М. : Академия, 2007. - 186,[1] с. - (Высшее профессиональное образование. Информационная безопасность). - Допущено УМО. - ISBN 978-5-7695-3098-2 : 150-70. Местонахождение: Научная библиотека ДГУ URL

2. Хорев, Павел Борисович. Методы и средства защиты информации в компьютерных системах : учеб. пособие для студентов вузов, обуч. по направлению 230100 (654600) "Информатика и вычисл. техника" / Хорев, Павел Борисович. - 3-е изд., стер. - М. : Академия, 2007. - 254,[1] с. - (Высшее профессиональное образование. Информатика и вычислительная техника). - Рекомендовано УМО. - ISBN 978-5-7695-4157-5 : 180-40. Местонахождение: Научная библиотека ДГУ URL

3. Петраков, Алексей Васильевич. Основы практической защиты информации : Учеб. пособие для вузов связи / Петраков, Алексей Васильевич. - 2-е изд. - М. : Радио и связь, 2000. - 361 с. - ISBN 5-256-01552-4 : 62-50. Местонахождение: Научная библиотека ДГУ URL:

9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины.

1. http://habrahabr.ru/
2. http://www.intuit.ru/

10. Методические указания для обучающихся по освоению дисциплины.

Студенты очной формы обучения нормативного срока обучения изучают дисциплину "Программно-аппаратные средства защиты информации" в течение 7 семестра. Виды и объем учебных занятий, формы контроля знаний приведены в табл. 1. Темы и разделы рабочей программы, количество лекционных часов и количество часов самостоятельной работы студентов на каждую из тем приведены в табл. 2. В первой колонке этой таблицы указаны номера тем согласно разделу 4. Организация лабораторного практикума, порядок подготовки к лабораторным занятиям и методические указания к самостоятельной работе студентов, а также порядок допуска к лабораторным занятиям и отчетности по проделанным работам определены в методических указаниях по выполнению лабораторных работ.

Самостоятельная работа студентов в ходе изучения лекционного материала заключается в проработке каждой темы в соответствии с методическими указаниями, а также в подготовке выполнения лабораторных работ, которые выдаются преподавателем на лекционных занятиях.

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем.

- Операционная система: Windows 7/8/Server 2008/ Server 2008 R2/ Server 2012**.**
- ПК виртуального моделирования сетей Cisco Packet Tracer 5.3.3.
- ПК редактирования документов Microsoft Word 2010.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

- Компьютерный класс;
- 15 компьютеров;
- Типы: Pentium IV или выше;
- Проектор с экраном.