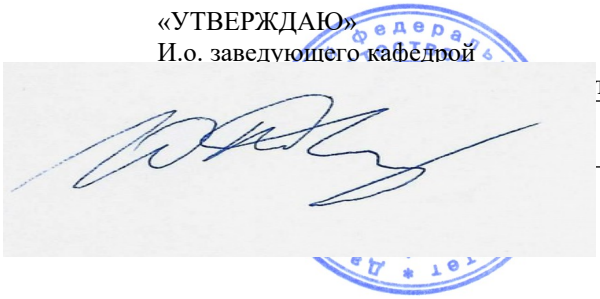
МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

«СОГЛАСОВАНО»
Руководитель ОП

Варлатая С.К.
(подпись) (Ф.И.О.)

«УТВЕРЖДАЮ»
И.о. заведующего кафедрой



ти

Ю.В.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (РПД)
«Защита на сетевом уровне»
Направление подготовки 10.03.01 «Информационная безопасность»
Профиль подготовки - «Комплексная защита объектов информатизации»
Форма подготовки очная

курс 4 семестр 8
лекции 18 час.
практические занятия 0 час.
лабораторные работы 18 час.
в том числе с использованием МАО лек. 00 / пр. 00 / лаб. 00 час.
всего часов аудиторной нагрузки 36 час.
в том числе с использованием МАО 00 час.
самостоятельная работа 72 час.
в том числе на подготовку к экзамену 0 час.
контрольные работы (количество) не предусмотрены
курсовая работа / курсовой проект не предусмотрены
зачет 8 семестр
экзамен не предусмотрен

Рабочая программа составлена в соответствии с требованиями образовательного стандарта, самостоятельно устанавливаемого ДВФУ, утвержденного приказом ректора от 20.07.2017 №12-13-1479.

Рабочая программа обсуждена на заседании кафедры информационной безопасности
протокол 10 о « 15 » июня 2019 г.
№ _____ т _____ _____

И.о. заведующего кафедрой : Добржинский Ю.В., к.т.н., с.н.с.
Составитель (ли): Зотов С.С., ассистент

Владивосток
2019

Оборотная сторона титульного листа РПД

I. Рабочая программа пересмотрена на заседании кафедры:

Протокол от «_____» _____ 20___ г. № _____

Заведующий кафедрой _____ _____

(подпись) (И.О. Фамилия)

II. Рабочая программа пересмотрена на заседании кафедры:

Протокол от «_____» _____ 20___ г. № _____

Заведующий кафедрой _____ _____

(подпись) (И.О. Фамилия)

III. Рабочая программа пересмотрена на заседании кафедры:

Протокол от «_____» _____ 20___ г. № _____

Заведующий кафедрой _____ _____

(подпись) (И.О. Фамилия)

IV. Рабочая программа пересмотрена на заседании кафедры:

Протокол от «_____» _____ 20___ г. № _____

Заведующий кафедрой _____ _____

(подпись) (И.О. Фамилия)

Аннотация к рабочей программе дисциплины

«Защита на сетевом уровне»

Рабочая программа дисциплины «Защита на сетевом уровне» разработана для студентов, обучающихся по направлению 10.03.01 «Информационная безопасность.

Общая трудоемкость освоения дисциплины составляет 108 часов (3 з.е.). Учебным планом предусмотрены лекционные занятия (18 час.), лабораторные работы (18 час.), самостоятельная работа студентов (72 час.). Дисциплина реализуется на 4 курсе в 8 семестре. Форма контроля по дисциплине – зачет.

Дисциплина «Защита на сетевом уровне» относится к базовой части профессионального цикла. Изучение дисциплины «Защита на сетевом уровне» базируется на следующих дисциплинах: «Вычислительные сети», «Защита информации в операционных системах», «Программно-аппаратные средства защиты информации».

Дисциплина «Защита на сетевом уровне» обеспечивает изучение следующих дисциплин: «Комплексная защита систем на предприятии». Знания и практические навыки, полученные из дисциплины «Защита на сетевом уровне», используются студентами при разработке курсовых и дипломных работ.

Целью дисциплины «Защита на сетевом уровне» является формирование у студентов знаний и умений по защите компьютерных сетей с применением современных программно-аппаратных средств.

Задачи:

1. Изучить методы и средства защиты информации в компьютерных сетях.

2. Изучить технологии межсетевого экранирования.

3. Изучить методы и средства построения виртуальных частных сетей.

4. Изучить методы и средства аудита уровня защищенности информационных систем.

В результате изучения данной дисциплины у обучающихся формируются следующие профессиональные компетенции (элементы компетенций).

Код и формулировка компетенции	**Этапы формирования компетенции**	
(ПК-16) способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	Знает	правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны
	Умеет	анализировать и оценивать угрозы информационной безопасности объекта
	Владеет	методами формирования требований по защите информации
(ПК-17) способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности	Знает	методы и принципы организационной защиты информации на предприятии
	Умеет	формулировать и настраивать политику безопасности распространенных систем, а также локальных вычислительных сетей, построенных на их основе
	Владеет	методами формирования требований по защите информации на предприятии

Для формирования вышеуказанных компетенций в рамках дисциплины «Защита на сетевом уровне» применяются следующие методы активного/ интерактивного обучения: интерактивные и проблемные лекции, лекции-диалоги, работа в малых группах, метод обучения в парах. Используемые оценочные средства: лабораторные работы (ПР-6), конспект (ПР-7).

I. СТРУКТУРА И СОДЕРЖАНИЕ ТЕОРЕТИЧЕСКОЙ ЧАСТИ КУРСА

МОДУЛЬ 1. Проблемы информационной безопасности (2 час.)

Раздел I. Основные понятия и анализ угроз информационной безопасности (2 час.)

Тема 1. Анализ угроз информационной безопасности в корпоративных системах и сетях (2 час.)

Содержание темы: Анализ угроз информационной безопасности. Анализ угроз корпоративных сетей. Тенденция развития ИТ-угроз. Криминализация атак на компьютерные сети и системы. Обеспечение информационной безопасности компьютерных систем.

МОДУЛЬ 2. Многоуровневая защита корпоративных информационных систем. (16 час.)

Раздел I. Протоколы защищенных каналов (5 час.)

Тема 1. Защита на канальном, сетевом и сеансовом уровнях (5 час.)

Содержание темы: Модель взаимодействия систем ISO/OSI и стек протоколов TCP/IP. Протоколы PPTP, L2TP, IPSec, SSL, TLS и SOCKS.

Раздел II. Технология межсетевого экранирования (6 час.)

Тема 1. Функции межсетевых экранов и особенности их функционирования на различных уровнях модели OSI (3 час.)

Содержание темы: Фильтрация трафика. Выполнение функции посредничества. Экранирующий маршрутизатор. Шлюз сеансового уровня. Прикладной шлюз. Шлюз экспертного уровня. Варианты исполнения межсетевых экранов.

Тема 2. Схемы сетевой защиты на базе межсетевых экранов (3 час.)

Содержание темы: Формирование политики межсетевого взаимодействия. Основные схемы подключения межсетевых экранов. Персональные и распределенные сетевые экраны. Примеры современных межсетевых экранов. Тенденции развития межсетевых экранов.

Раздел III. Организация виртуальных частных сетей (4 час.)

Тема 1. Концепция построения виртуальных защищенных сетей VPN (2 час.)

Содержание темы: Основные понятия и функции сети VPN. Варианты построения виртуальных защищенных каналов. Средство обеспечения безопасности VPN.

Тема 2. VPN - решения для построения защищенных сетей (2 час.)

Содержание темы: Классификация сетей VPN. Основные варианты архитектуры VPN. Основные виды технической реализации VPN.

Раздел IV. Технологии обнаружения и предотвращения вторжений (1 час.)

Тема 1. Предотвращений вторжений в КИС (1 час.)

Содержание темы: Обнаружение вторжений системой IPS. Предотвращение вторжений системного уровня. Предотвращение вторжений сетевого уровня. Защита от DDoS-атак.

II. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКОЙ ЧАСТИ КУРСА

Лабораторные работы (18 час.)

Лабораторная работа №1. Применение межсетевого экрана на основе двудомного узла и на основе фильтрующего маршрутизатора (4 час.)

Лабораторная работа №2. Организация VPN средствами протокола PPTP (4 час.)

Лабораторная работа №3 Организация VPN средствами СЗИ VipNet (3 час.)

Лабораторная работа №4. Шифрование трафика с использованием протокола IPSec (4 час.)

Лабораторная работа №5. Организация VPN средствами СЗИ StrongNet (3 час.)

III. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине «Электроника и схемотехника» представлено в Приложении 1 и включает в себя:

- план-график выполнения самостоятельной работы по дисциплине, в том числе примерные нормы времени на выполнение по каждому заданию;
- характеристика заданий для самостоятельной работы обучающихся и методические рекомендации по их выполнению;
- требования к представлению и оформлению результатов самостоятельной работы.

IV. КОНТРОЛЬ ДОСТИЖЕНИЯ ЦЕЛЕЙ КУРСА

№ п/п	Контролируемые разделы / темы дисциплины	Коды и этапы формирования компетенций		Оценочные средства - наименование	
				текущий контроль	промежуточная аттестация
1	МОДУЛЬ 1. Проблемы информационной безопасности	ПК-16, ПК-17	знает	ПР-1	1-11
			умеет	ПР-7	1-11
			владеет	ПР-4	1-11
2	МОДУЛЬ 2. Многоуровневая защита корпоративных информационных систем	ПК-16, ПК-17	знает	ПР-7	12-22
			умеет	ПР-7	12-22
			владеет	ПР-6	12-22

Методические материалы, определяющие процедуры оценивания знаний, умений и навыков и (или) опыта деятельности, а также критерии характеризующие этапы формирования компетенций в процессе освоения образовательной программы, представлены в Приложении 2.

V. СПИСОК УЧЕБНОЙ ЛИТЕРАТУРЫ И ИНФОРМАЦИОННО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература

(электронные и печатные издания)

1. Компьютерные сети : учеб. пособие / А.В. Кузин, Д.А. Кузин. — 4-е изд., перераб. и доп. — М. : ФОРУМ : ИНФРА-М, 2018. — 190 с. —

(Среднее профессиональное образование). - Режим доступа: http://znanium.com/catalog/product/938938

2. В. Г. Олифер, Н. А. Олифер «Компьютерные сети. Принципы, технологии, протоколы» 5-е издание СПб.: Питер, 2015, 943 с. http://lib.dvfu.ru:8080/lib/item?id=chamo:794589&theme=FEFU

3. Комплексная защита информации в корпоративных системах : учеб. пособие / В.Ф. Шаньгин. — М. : ИД «ФОРУМ» : ИНФРА-М, 2017. — 592 с. — (Высшее образование: Бакалавриат). – Режим доступа: http://znanium.com/catalog/product/546679

Дополнительная литература

(печатные и электронные издания)

1. Компьютерные сети: Учебное пособие / Н.В. Максимов, И.И. Попов. - 3-е изд., испр. и доп. - М.: Форум, 2008. - 448 с.: ил.; 60x90 1/16. - (Профессиональное образование). (переплет) ISBN 978-5-91134-235-7 - Режим доступа: http://znanium.com/catalog/product/163728

2. Васин Н.Н. Основы конфигурирования коммутаторов и маршрутизаторов Huawei [Электронный ресурс]: методические указания по проведению лабораторных работ/ Васин Н.Н., Вьюшкова Е.А.— Электрон. текстовые данные.— Самара: Поволжский государственный университет телекоммуникаций и информатики, 2016.— 54 c.— Режим доступа: http://www.iprbookshop.ru/71863.html.— ЭБС «IPRbooks»

3. Компьютерные сети: Учебное пособие / Н.В. Максимов, И.И. Попов. - 3-е изд., испр. и доп. - М.: Форум, 2008. - 448 с.: ил.; 60x90 1/16. - (Профессиональное образование). (переплет) ISBN 978-5-91134-235-7 - Режим доступа: http://znanium.com/catalog/product/163728

Интернет-ресурсы:

1. https://www.twirpx.com/file/1509899/ - Бройдо В.Л. Вычислительные системы сети и телекоммуникации. – СПб.: Питер, 2011. – 506 с.

2. Компьютерные сети: Учебное пособие / А.В. Кузин. - 3-е изд., перераб. и доп. - М.: Форум: НИЦ ИНФРА-М, 2014. - 192 с: http://znanium.com/catalog/product/450375

3. http://www.knigafund.ru/books/42544 / Чекмарев Ю.В. «Локальные вычислительные сети» Издательство: ДМК Пресс, 2009, 200 с.

Перечень информационных технологий и программного обеспечения

Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 738, Учебная аудитория для проведения занятий лекционного, практического и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	1) IBM SPSS Statistics Premium Campus Edition. Поставщик ЗАО Прогностические решения. Договор ЭА-442-15 от 18.01.16 лот 5. Срок действия договора 30.06.2016. Лицензия бессрочно. 2) SolidWorks Campus 500. Поставщик Солид Воркс Р. Договор 15-04-101 от 23.12.2015. Срок действия договора 15.03.2016. Лицензия бессрочно. 3) АСКОН Компас 3D v17. Поставщик Навиком. Договор 15-03-53 от 20.12.2015. Срок действия договора 31.12.2015. Лицензия бессрочно. 4) MathCad Education Universety Edition. Поставщик Софт Лайн Трейд. Договор 15-03-49 от 02.12.2015. Срок действия договора 30.11.2015. Лицензия бессрочно. 5) Corel Academic Site. Поставщик Софт Лайн Трейд. Договор ЭА-442-15 от 18.01.16 лот 4. Срок действия договора 30.06.2016. Лицензия закончилась 28.01.2019. 6) Microsoft Office, Microsoft Visual Studio. Поставщик Софт Лайн Трейд. Договор ЭА-261-18 от 02.08.18 лот 4. Срок действия договора 20.09.2018. Лицензия до 30.06.2020.
Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 734, Компьютерный класс, аудитория для проведения занятий лекционного, практического и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	1) IBM SPSS Statistics Premium Campus Edition. Поставщик ЗАО Прогностические решения. Договор ЭА-442-15 от 18.01.16 лот 5. Срок действия договора 30.06.2016. Лицензия бессрочно. 2) SolidWorks Campus 500. Поставщик Солид Воркс Р. Договор 15-04-101 от 23.12.2015. Срок действия договора 15.03.2016. Лицензия бессрочно. 3) АСКОН Компас 3D v17. Поставщик Навиком. Договор 15-03-53 от 20.12.2015. Срок действия договора 31.12.2015. Лицензия бессрочно. 4) MathCad Education Universety Edition. Поставщик Софт Лайн Трейд. Договор 15-03-49 от 02.12.2015. Срок действия договора 30.11.2015. Лицензия бессрочно. 5) Corel Academic Site. Поставщик Софт Лайн Трейд. Договор ЭА-442-15 от 18.01.16 лот 4. Срок действия договора 30.06.2016. Лицензия закончилась 28.01.2019. 6) Microsoft Office, Microsoft Visual Studio. Поставщик Софт Лайн Трейд. Договор ЭА-261-18 от 02.08.18 лот 4.

	Срок действия договора 20.09.2018. Лицензия до 30.06.2020.
Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 733, Компьютерный класс, аудитория для проведения занятий лекционного, практического и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	1) IBM SPSS Statistics Premium Campus Edition. Поставщик ЗАО Прогностические решения. Договор ЭА-442-15 от 18.01.16 лот 5. Срок действия договора 30.06.2016. Лицензия бессрочно. 2) SolidWorks Campus 500. Поставщик Солид Воркс Р. Договор 15-04-101 от 23.12.2015. Срок действия договора 15.03.2016. Лицензия бессрочно. 3) АСКОН Компас 3D v17. Поставщик Навиком. Договор 15-03-53 от 20.12.2015. Срок действия договора 31.12.2015. Лицензия бессрочно. 4) MathCad Education Universety Edition. Поставщик Софт Лайн Трейд. Договор 15-03-49 от 02.12.2015. Срок действия договора 30.11.2015. Лицензия бессрочно. 5) Corel Academic Site. Поставщик Софт Лайн Трейд. Договор ЭА-442-15 от 18.01.16 лот 4. Срок действия договора 30.06.2016. Лицензия закончилась 28.01.2019. 6) Microsoft Office, Microsoft Visual Studio. Поставщик Софт Лайн Трейд. Договор ЭА-261-18 от 02.08.18 лот 4. Срок действия договора 20.09.2018. Лицензия до 30.06.2020.

VI. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Количество аудиторных часов, отведенных на изучение дисциплины «Защита на сетевом уровне», составляет 72 часа. На самостоятельную работу – 36 часов. При этом аудиторная нагрузка состоит из 36 лекционных часов и 36 часов лабораторных работ.

Обучающийся получает теоретические знания на лекциях. В ходе подготовки к лекциям должны использоваться источники из списка учебной литературы.

Подготовка к лабораторным работам предполагает повторение лекционного материала. В результате студент должен быть готов к выполнению лабораторных работ. Основной лабораторных работ является выполнение заданий с последующим предоставлением отчета о выполнении.

В рамках указанной дисциплины итоговой формы аттестации является зачет. Самостоятельная работа при подготовке к зачету включает изучение

теоретического материала с использованием лекционных материалов, рекомендуемых источников и материалов лабораторных работ.

VII. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 738, Учебная аудитория для проведения занятий лекционного, практического и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	Помещение укомплектовано специализированной учебной мебелью (посадочных мест – 208) Оборудование: Мультимедийное оборудование: Экран проекционный Projecta Elpro Large Electrol, 500x316 см, размер рабочей области 490x306 Документ-камера Avervision CP 355 AF Мультимедийный проектор Panasonic PT-DZ11OXE, 10 600 ANSI Lumen, 1920x1200 Сетевая видеокамера Multipix MP-HD718 ЖК-панель 47", Full HD, LG M4716 CCBA ЖК-панель 42", Full HD, LG M4214 CCBA ЖК-панель 42", Full HD, LG M4214 CCBA Доска аудиторная, переносной компьютер (ноутбук Lenovo) с сумкой – 1 шт.
Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 734, Компьютерный класс, аудитория для проведения занятий лекционного, практического и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	Помещение укомплектовано специализированной учебной мебелью (посадочных мест – 15) Оборудование: "Моноблок HPP-B0G08ES#ACB/8200E AIO i52400S 500G 4.0G 28 PC Мультимедийное оборудование: Экран проекционный ScreenLine Trim White Ice 50 см черная кайма сверху, размер рабочей области 236x147 см Документ-камера Avervision CP355AF ЖК-панель 47"", Full HD, LG M4716 CCBA Мультимедийный проектор Mitsubishi EW33OU, 3000 ANSI Lumen, 1280x800 Сетевая видеокамера Multipix MP-HD718 " Доска аудиторная
Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 733,	Помещение укомплектовано специализированной учебной мебелью (посадочных мест – 15)

Компьютерный класс, аудитория для проведения занятий лекционного, практического и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	Оборудование: "Моноблок lenovo C360G-i34164G500UDK Мультимедийное оборудование: Экран проекционный ScreenLine Trim White Ice 50 см черная кайма сверху, размер рабочей области 236x147 см Документ-камера Avervision CP355AF ЖК-панель 47"", Full HD, LG M4716 CCBA Мультимедийный проектор Mitsubishi EW33OU, 3000 ANSI Lumen, 1280x800 Сетевая видеокамера Multipix MP-HD718" Доска аудиторная

Приложение 1

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ
по дисциплине «Защита на сетевом уровне»
Направление подготовки 10.03.01 Информационная безопасность
профиль «Комплексная защита объектов информатизации»
Форма подготовки очная

Владивосток
2019

План-график выполнения самостоятельной работы по дисциплине

№ п/п	Дата/сроки выполнения	Вид самостоятельной работы	Примерные нормы времени на выполнение	Форма контроля
1	1-18 неделя обучения	Подготовка лабораторных работ.	48	Отчет о выполнении
2	Сессия	Подготовка к зачету	24	Зачет

Подготовка отчетов к лабораторным работам предполагает повторение лекционного материала и выполнение лабораторных работ. В результате студент должен представить отчеты о проделанной работе.

Большое значение в процессе обучения имеет самостоятельная работа студентов, на которую отводится значительная часть часов учебного плана. Самостоятельная работа студентов ведется под контролем преподавателя и

включает работу с конспектами лекций и литературой, теоретическую подготовку к выполнению лабораторных работ и их защите, оформление лабораторно-практических работ, подготовку к контрольным занятиям.

Критерии оценки выполнения самостоятельной работы

Контроль самостоятельной работы студентов предусматривает:

- соотнесение содержания контроля с целями обучения;
- объективность контроля;
- валидность контроля (соответствие предъявляемых заданий тому, что предполагается проверить);
- дифференциацию контрольно-измерительных материалов.

Формы контроля самостоятельной работы

1. Просмотр и проверка выполнения самостоятельной работы преподавателем.
2. Самопроверка, взаимопроверка выполненного задания в группе.
3. Обсуждение результатов выполненной работы на занятии.
4. Текущее тестирование.

Критерии оценки результатов самостоятельной работы

Критериями оценок результатов внеаудиторной самостоятельной работы студента являются:

- уровень освоения студентов учебного материала;
- умения студента использовать теоретические знания при выполнении практических задач;
- умения студента активно использовать электронные образовательные ресурсы, находить требующуюся информацию, изучать ее и применять на практике;
- обоснованность и четкость изложения ответа;
- оформление материала в соответствии с требованиями;

- умение ориентироваться в потоке информации, выделять главное;
- умение четко сформулировать проблему, предложив ее решение, критически оценить решение и его последствия;
- умение показать, проанализировать альтернативные возможности, варианты действий;
- умение сформировать свою позицию, оценку и аргументировать ее.

Критерии оценки выполнения контрольных заданий для самостоятельной работы

Процент правильных ответов	**Оценка**
От 95% до 100%	отлично
От 76% до 95%	хорошо
От 61% до 75%	удовлетворительно
Менее 61 %	неудовлетворительно

Самостоятельная работа при подготовке к зачету включает изучение теоретического материала с использованием лекционных материалов, рекомендуемых источников, материалов по практическим занятиям и лабораторным работам.

Приложение 2

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
по дисциплине «Защита на сетевом уровне»
Направление подготовки 10.03.01 Информационная безопасность
профиль «Комплексная защита объектов информатизации»
Форма подготовки очная

Владивосток
2019

Паспорт фонда оценочных средств

Код и формулировка компетенции	Этапы формирования компетенции	
способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации (ПК-16);	Знает	Правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны
	Умеет	Анализировать и оценивать угрозы информационной безопасности объекта
	Владеет	Методами формирования требований по защите информации
способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности (ПК-17).	Знает	Методы и принципы организационной защиты информации на предприятии
	Умеет	Формулировать и настраивать политику безопасности распространенных систем, а также локальных вычислительных сетей, построенных на их основе
	Владеет	Методами формирования требований по защите информации на предприятии

Контроль достижения целей курса

№ п/п	Контролируемые разделы / темы дисциплины	Коды и этапы формирования компетенций		Оценочные средства - наименование	
				текущий контроль	промежуточная аттестация
1	МОДУЛЬ 1. Проблемы информационной безопасности	ПК-16, ПК-17	знает	ПР-1	1-11
			умеет	ПР-7	1-11
			владеет	ПР-4	1-11
2	МОДУЛЬ 2. Многоуровневая защита корпоративных информационных систем	ПК-16, ПК-17	знает	ПР-7	12-22
			умеет	ПР-7	12-22
			владеет	ПР-6	12-22

Оценочные средства для промежуточной аттестации
Список вопросов на зачет

1. Атаки на протоколы и службы Интернет. Методы и средства защиты.

2. Понятие межсетевых экранов. Компоненты межсетевого экрана. Политика сетевой безопасности.

3. Критерии фильтрации пакетов. Основные схемы сетевой защиты на базе межсетевых экранов.

4. Создание защищенных сегментов сетей с использованием межсетевых экранов.

5. Конфигурирование сетевых фильтров на базе настроек безопасности протокола TCP/IP в ОС Windows XP.

6. Защита рабочих станций с использованием персональных сетевых фильтров.

7. Организация VPN-сетей. Задачи, решаемые VPN. Туннелирование в VPN.

8. Электронные сертификаты. Понятие инфраструктуры открытых ключей.

9. Протоколы и средства организации VPN на сетевом уровне. Назначение, область применения, аутентификация и шифрование данных в протоколах SKIP и IPSec.

10. Протоколы PPTP, SSL. Назначение, область применения, аутентификация и шифрование данных.

11. Преимущества технологии терминального доступа. Обеспечение безопасности.

12. Назначение систем обнаружения атак. Классификация систем обнаружения атак.

13. Службы каталогов. Общие сведения о службах каталогов. Структура каталога LDAP.

14. Система единого входа в сеть на основе протокола Kerberos. Создание единого пространства безопасности на базе Active Directory.

15. Аудит безопасности компьютерных систем. Цели, стандарты, подходы.

16. Инструментальные средства аудита безопасности компьютерных систем, их возможности и недостатки. Применение инструментальных средств аудита безопасности компьютерных систем.

17. Тестирование состояния защищенности компьютерных систем от

18. несанкционированного доступа с использованием сканеров безопасности. Методика проведения инструментальных проверок.

19. Классификация средств и информационных ресурсов в соответствии со стандартом ISO-17799.

20. Назначение и основные функции программных комплексов «Гриф-специалист» и «Кондор-специалист». Построение модели защиты компьютерной системы с использованием комплексной экспертной системы «АванГард».

21. Виды требований безопасности согласно ГОСТ Р ИСО/МЭК 15408-1-2002. «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий».

22. Назначение систем обнаружения атак. Классификация систем обнаружения атак. Использование системы обнаружения атак «Snort».