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

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

«СОГЛАСОВАНО»
Руководитель ОП
«Информационная безопасность»
_____ Варлатая С.К.
(подпись) (Ф.И.О. рук. ОП)
« 5 » июля 2018 г.

«УТВЕРЖДАЮ»
Заведующий (ая) кафедрой
информационной безопасности
(название кафедры)
_____ Добржинский Ю.В.
(подпись) (Ф.И.О. рук. ОП)
« 5 » июля 2018 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ (РПУД)
«Защита информационных процессов в компьютерных системах»
Направление –10.03.01 «Информационная безопасность»
Профиль подготовки - «Комплексная защита объектов информатизации»
Форма подготовки – очная

курс 4 семестр 7
лекции 36 час.
практические занятия 0 час.
лабораторные работы 36 час.
в том числе с использованием МАО лек. ____ / пр. ____ / лаб. ____ час.
всего часов аудиторной нагрузки 72 час.
в том числе с использованием МАО ____ час.
самостоятельная работа 36 час.
в том числе на подготовку к экзамену 36 час.
контрольные работы (количество) учебным планом не предусмотрены
курсовая работа / курсовой проект учебным планом не предусмотрены
зачет учебным планом не предусмотрен
экзамен 7 семестр

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 от « 15 » июня 2019 г.

Заведующий (ая) кафедрой: Добржинский Ю.В., к.т.н., с.н.с.
Составитель (ли): Корнюшин П.Н., д.т.н., профессор

I. Рабочая программа пересмотрена на заседании кафедры:

Протокол от «_____» _____ 20 г. № _____

Заведующий кафедрой _____ _Ю.В. Добржинский_
(подпись) (и.о. фамилия)

II. Рабочая программа пересмотрена на заседании кафедры:

Протокол от «_____» _____ 200 г. № _____

Заведующий кафедрой _____ _Ю.В. Добржинский_
(подпись) (и.о. фамилия)

Аннотация к рабочей программе дисциплины
«Защита информационных процессов в компьютерных системах»

Дисциплины «Защита информационных процессов в компьютерных системах» является теоретической и практической подготовкой специалистов к деятельности по осуществлению анализа защищенности компьютерных систем (КС), принципам формального моделирования и анализа безопасности КС, реализующих управление доступом и информационными потоками, а также содействие фундаментализации образования, формированию научного мировоззрения и развитию системного мышления.

Общая трудоемкость освоения дисциплины составляет 144 часа (4 з.е.). Учебным планом предусмотрены лекционные занятия (36 час.), лабораторные работы (36 час.), самостоятельная работа студентов (36 час.), контроль качества обучения студентов (36 час.). Дисциплина реализуется на 4 курсе в 7 семестре. Форма контроля по дисциплине – экзамен.

Цель: изучить основные виды политик управления доступом и информационными потоками в КС в том числе и основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков.

Задачи:

- изучение основных формальных моделей политик безопасности, моделей дискреционного, мандатного, ролевого управления доступом, изолированной программной среды и безопасности информационных потоков;

- приобретение навыков использования математических моделей безопасности при осуществлении анализа защищенности КС.

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

Код и формулировка компетенции	Этапы формирования компетенции	
(ПК-2) способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	Знает	программные средства системного, прикладного и специального назначения для защиты информации, а так же современные инструментальные средства, языки и системы программирования
	Умеет	применять для различных целей программные средства системного, прикладного и специального назначения
	Владеет	современными и широко используемыми языками и системами программирования для решения профессиональных задач
(ПК-8) способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	Знает	принципы и методы проектирования подсистем и средств обеспечения информационной безопасности
	Умеет	применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности систем
	Владеет	методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов и технико-экономической экспертизы
(ПК-9) способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	Знает	основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, федеральной службы по техническому и экспортному контролю в данной области
	Умеет	пользоваться нормативными и техническими документами по защите информации
	Владеет	навыками работы с нормативными правовыми актами, способностью оформлять рабочую техническую документацию
(ПК-11) способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять	Знает	основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области

обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	Умеет	применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем
	Владеет	профессиональной терминологией и навыками работы с нормативными правовыми актами

Для формирования вышеуказанных компетенций в рамках дисциплины «Защита информационных процессов в компьютерных системах» 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. Классификация угроз, понятия. (16 ч)

Раздел 1. Введение. Основные понятия и определения. (16 ч)

Тема 1. Сущность, субъект, доступ, информационный поток (7 ч)

Основные элементы теории компьютерной безопасности (сущность, субъект, доступ, право доступа, информационные потоки по памяти или по времени). Основная аксиома. Проблема построения защищенной КС. Модели ценности информации: аддитивная модель, порядковая шкала, решетка многоуровневой безопасности.

Тема 2. Угрозы безопасности информации. Политика безопасности (9ч)

Классификация угроз безопасности информации. Угрозы конфиденциальности, целостности, доступности информации, раскрытия параметров КС. Понятие политики безопасности. Модель нарушителя. Основные виды политик управления доступом и информационными потоками. Политики дискреционного, мандатного, ролевого управления

доступом, изолированной программной среды и безопасности информационных потоков.

Модуль 2. Виды моделей разграничения доступа. (20ч)

Раздел 1. Модели компьютерных систем с дискреционным управлением доступом (20 ч)

Тема 1. Модель матрицы доступов Харрисона-Руззо-Ульмана (7 ч)

Модель матрицы доступов Харрисона-Руззо-Ульмана (ХРУ). Анализ безопасности систем ХРУ. Монооперационные системы ХРУ. Алгоритмическая неразрешимость задачи проверки безопасности систем ХРУ.

Тема 2. Классическая и расширенная модели распространения прав доступа Take-Grant (7 ч)

Классическая модель Take-Grant. Де-юре правила преобразования графов доступов. Условия передачи прав доступа в графе доступов, состоящем только из субъектов. Остров, мост, пролеты моста. Условия передачи прав доступа в произвольном графе доступов при отсутствии ограничений на кооперацию субъектов. Элементы расширенной модели Take-Grant. Де-факто правила преобразования графов доступов и информационных потоков.

Тема 3. Субъектно-ориентированная модель изолированной программной среды (6 ч)

Субъектно-ориентированная модель изолированной программной среды (ИПС). Объекты, функционально ассоциированные с субъектами. Мониторы безопасности обращений и порождения субъектов. Базовая теорема ИПС.

II. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКОЙ ЧАСТИ КУРСА

Лабораторная работа (36ч)

Тема 1. Основные угрозы информации в компьютерных системах (6ч)

Тема 2. Специфика возникновения угроз в открытых сетях (6ч)

Тема 3. Особенности защиты информации на узлах компьютерной сети с использованием криптографических методов (6ч)

Тема 4. Администрирование серверных систем и приложений (6ч)

Тема 5. Использование межсетевых экранов для защиты информационных процессов (5ч)

Тема 6. Требования к защите автоматизированных систем от НСД (7ч)

III. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине «Защита информационных процессов в компьютерных системах» 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. Классификация угроз, понятия.	ПК-2, ПК-8, ПК-9, ПК-11	знает	ПР-1	1-28
			умеет	ПР-7	1-28
			владеет	ПР-6	1-28

2	Модуль 2. Виды моделей разграничения доступа	ПК-2, ПК-8, ПК-9, ПК-11	знает	ПР-1	29-39
			умеет	ПР-7	29-39
			владеет	ПР-6	29-39

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. Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. Учебное пособие для вузов. М.: Горячая линия - Телеком, 2011. 320 с. http://lib.dvfu.ru:8080/lib/item?id=chamo:263487&theme=FEFU

2. Аппаратно-программные средства защиты информации: Практикум / Душкин А.В., Дубровин А.С., Здольник В.В. - Воронеж:Научная книга, 2017. - 198 с.: ISBN 978-5-4446-1043-5 - Режим доступа: http://znanium.com/catalog/product/977192

3. Безопасность и управление доступом в информационных системах: учеб. пособие / А.В. Васильков, И.А. Васильков. — М.: ФОРУМ: ИНФРА-М, 2017. — 368 с. — (Среднее профессиональное образование). - Режим доступа: http://znanium.com/catalog/product/537054

4. Грибунин, В. Г. Комплексная система защиты информации на предприятии: учеб. пособие для вузов по спец. "Орг. и технология защиты информации", "Комплекс. защита объектов информатизации" / В. Г. Грибунин, В. В. Чудовский. - М.: Академия, 2009. - 412 с.: ил., табл. - (Высшее профессиональное образование. Информационная безопасность). - Библиогр.: с. 403-406. http://lib.dvfu.ru:8080/lib/item?id=chamo:290528&theme=FEFU

5. 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

6. А. И. Куприянов, А. В. Сахаров, В. А. Шевцов / Основы защиты информации : учебное пособие Москва : Академия, 2008. – 254 с. - http://lib.dvfu.ru:8080/lib/item?id=chamo:382044&theme=FEFU, 2008, стр. -] - Режим доступа: http://znanium.com/catalog/product/524693

Дополнительная литература

(печатные и электронные издания)

1. Нестеров С.А., Основы информационной безопасности [Электронный ресурс] : учебное пособие / Нестеров С.А.. — Электрон. текстовые данные. — СПб. : Санкт-Петербургский политехнический университет Петра Великого, 2014. — 322 c. — 978-5-7422-4331-1. — Режим доступа: http://www.iprbookshop.ru/43960.html

2. Щербаков А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. Учебное пособие. М.: Книжный мир, 2010. 380 с. http://lib.dvfu.ru:8080/lib/item?id=chamo:706509&theme=FEFU

3. Белов Е.Б. Основы информационной безопасности. Учебное пособие для вузов. – М.: Горячая линия-Телеком, 2006. — 544 с. http://lib.dvfu.ru:8080/lib/item?id=chamo:262748&theme=FEFU

Интернет-ресурсы

1. http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=4925 Пушкарев В.В. Пушкарев В.П. Защита информационных процессов в компьютерных системах. 2012г. 131 стр.

2. http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=6031 Горенский Б.М.Кирякова О.В.Лапина Л.А.Ченцов С.В. Информационные технологии в управлении технологическими процессами цветной металлургии: лабораторный практикум. 2012г. 148 стр.

3. http://telecomlaw.ru/studyguides/is_varfolomeev.pdf Варфоломеев А.А. «Основы информационной безопасности: Учеб. пособие. – М.: РУДН, 2008. – 412 с.: ил.

Перечень информационных технологий и программного обеспечения

Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 318, Компьютерный класс кафедры информационной безопасности, 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. 7) Dallas Lock. Поставщик Конфидент. Партнерское соглашение БП-8-16/576-16-ЦЗ/1 от 23.11.2016. Срок действия договора 23.11.2019. Лицензия до 23.11.2019

VI. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Количество аудиторных часов, отведенных на изучение дисциплины «Защита информационных процессов в компьютерных системах», составляет 72 часа. На самостоятельную работу – 72 час. 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 экзамен. Самостоятельная работа при подготовке к экзамену включает изучение теоретического материала с использованием лекционных материалов, рекомендуемых источников и материалов лабораторных работ.

Методические указания для написания реферата

Прежде всего, нужно выбрать тему реферата и подобрать соответствующую литературу. После ознакомления с литературой следует приступить к составлению плана. План реферата должен состоять из названия (темы), введения, основной части, заключения и списка использованной литературы (3-5 работ). Основная часть, как правило, разбивается на дополнительные вопросы (не более 3-4).

Объём реферата должен быть не менее 12 машинописных страниц.

Во введении описывается цель, задачи работы, а также раскрываются смысл и значение основных понятий выбранной темы, область их применения.

В основной части необходимо:

а) ещё раз уточнить тему работы;

б) разбить основную часть работы на дополнительные вопросы;

в) дать ответы на эти вопросы, получив вспомогательные результаты. На их основе дать ответ на основной вопрос. Допускаются ссылки на дополнительную литературу.

В заключении подводятся итоги исследования. Заключение не должно быть большим по объёму.

VII. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 318, Компьютерный класс кафедры информационной безопасности, 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 Электронная доска Poly Vision Walk-and-Talk WTL 1810 Мультимедийная аудитория: 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 информационных процессов в компьютерных системах»

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 самостоятельных и лабораторных работ.	45	Отчет о выполнении
2	Сессия	Подготовка к экзамену	27	Экзамен

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

Методические рекомендации к работе с литературными источниками

В процессе подготовки к практическим занятиям, студентам необходимо обратить особое внимание на самостоятельное изучение рекомендованной учебно-методической (а также научной и популярной) литературы. Самостоятельная работа с учебниками, учебными пособиями, научной, справочной и популярной литературой, материалами периодических изданий и Интернета, статистическими данными является наиболее эффективным методом получения знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у студентов свое отношение к конкретной проблеме. Более глубокому раскрытию вопросов способствует знакомство с дополнительной литературой, рекомендованной преподавателем по каждой теме практического занятия, что позволяет студентам проявить свою индивидуальность в рамках выступления на данных занятиях, выявить широкий спектр мнений по изучаемой проблеме.

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 экзамену включает изучение теоретического материала с использованием лекционных материалов, рекомендуемых источников, материалов по 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 информационных процессов в компьютерных системах»

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	
способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач (ПК-2)	Знает	Программные средства системного, прикладного и специального назначения для защиты информации, а так же современные инструментальные средства, языки и системы программирования
	Умеет	Применять для различных целей программные средства системного, прикладного и специального назначения
	Владеет	Современными и широко используемыми языками и системами программирования для решения профессиональных задач
способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений (ПК-8)	Знает	Принципы и методы проектирования подсистем и средств обеспечения информационной безопасности
	Умеет	Применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности систем
	Владеет	Методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов и технико-экономической экспертизы
способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов (ПК-9)	Знает	Основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, федеральной службы по техническому и экспортному контролю в данной области
	Умеет	Пользоваться нормативными и техническими документами по защите информации
	Владеет	Навыками работы с нормативными правовыми актами, способностью оформлять рабочую техническую документацию
способностью осуществлять подбор, изучение и обобщение	Знает	Принципы организации информационных систем в соответствии с требованиями по защите информации

научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности (ПК-11)	Умеет	Пользоваться нормативными документами за защите информации
	Владеет	Навыками работы с нормативными правовыми актами

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. Классификация угроз, понятия.	ПК-2, ПК-8, ПК-9, ПК-11	знает	ПР-1	1-28
			умеет	ПР-7	1-28
			владеет	ПР-6	1-28
2	Модуль 2. Виды моделей разграничения доступа	ПК-2, ПК-8, ПК-9, ПК-11	знает	ПР-1	29-39
			умеет	ПР-7	29-39
			владеет	ПР-6	29-39

Оценочные средства для промежуточной аттестации

Список вопросов на экзамен

1. Представьте классификацию видов угроз информационной безопасности Российской Федерации. Перечислите угрозы безопасности информационных и телекоммуникационных средств и систем.

2. Какие функциональные блоки включает система разграничения доступа, нарисуйте структурную схему диспетчера доступа.

3. Представьте модель защиты доступа к компьютерной сети. Перечислите службы (функции) защиты компьютерной сети, дайте им определение.

4. Представьте структурно (рисунком) модели многозвенной и многоуровневой защиты информации и поясните их.

5. Представьте модель защиты компьютерной системы, какие составляющие имеет технология защиты информации и какие основные задачи необходимо решить при разработке конкретного средства защиты информации для этой модели.

6. На какие вопросы должна давать ответы политика безопасности предприятия?

7. Перечислите (представьте рисунками) виды нарушений в компьютерных системах и дайте им определение. Представьте классификацию нарушений в терминах пассивных и активных атак.

8. Перечислите (представьте структурно на рисунке) методы обеспечения безопасности процессов переработки информации, составляющих основу механизмов защиты в компьютерных системах. Какие функции защиты информации включает метод управления доступом.

9. Представьте классификацию методов и средств предотвращения угроз шпионажа и диверсий. Поясните применение системы охраны объекта и противодействие подслушиванию.

10. Перечислите базовые технологии (механизмы) безопасности информации в компьютерных системах. Дайте определение процессам идентификации, аутентификации и авторизации для обеспечения защиты информации.

11. Представьте классификацию методов и средств предотвращения угроз шпионажа и диверсий. Поясните организацию работы с конфиденциальными информационными ресурсами, противодействие наблюдению и защиту от злоумышленных действий обслуживающего персонала и пользователей компьютерной системы.

12. Перечислите базовые технологии (механизмы) безопасности информации в компьютерных системах. Дайте определение технологии защищенного канала.

13. Представьте классификацию методов предотвращения угроз несанкционированного доступа в компьютерных системах.

14. Перечислите (представьте структурно на рисунке) атаки на политику безопасности и процесс административного управления в компьютерной системе.

15. Перечислите формальные и неформальные средства обеспечения безопасности процессов переработки информации, составляющих основу механизмов защиты в компьютерных системах.

16. Каким требованиям должна удовлетворять безопасная информационная система.

17. Представьте классификацию методов и средств предотвращения случайных угроз компьютерных систем.

18. В чем заключается концепция построения виртуальных защищенных сетей VPN. Как формируется сеть VPN, дайте определение ей и ее основным устройствам, приведите пример пакета, подготовленного для туннелирования.

19. Представьте классификацию криптографических методов предотвращения угроз информационной безопасности в компьютерных системах. Каким требованиям должны отвечать современные методы шифрования.

20. Перечислите (представьте структурно на рисунке) атаки на постоянные компоненты системы защиты информации в компьютерной системе.

21. На какие группы подразделяются методы и средства парирования угроз информационной безопасности в компьютерных системах, представьте классификацию методов и средств парирования угроз от электромагнитных излучений и наводок. Поясните активные методы парирования угроз от электромагнитных излучений и наводок.

22. Перечислите (представьте структурно на рисунке) атаки на сменные элементы системы защиты информации в компьютерной системе.

23. На какие группы подразделяются методы и средства парирования угроз информационной безопасности в компьютерных системах, представьте классификацию методов и средств парирования угроз от электромагнитных излучений и наводок. Поясните пассивные методы парирования угроз от электромагнитных излучений и наводок.

24. Перечислите (представьте структурно на рисунке) атаки на протоколы информационного взаимодействия в компьютерной системе.

25. На какие группы подразделяются методы и средства нейтрализации угроз информационной безопасности в компьютерных системах, представьте классификацию методов и средств борьбы с компьютерными вирусами. В чем заключаются методы: сканирования, обнаружения изменений и эвристический анализ для поиска вирусов.

26. Перечислите (представьте структурно на рисунке) нападения на функциональные элементы компьютерных сетей.

27. На какие группы подразделяются методы и средства нейтрализации угроз информационной безопасности в компьютерных системах, представьте классификацию методов и средств борьбы с компьютерными вирусами. В чем заключаются методы использования резидентных сторожей и аппаратно-программной защиты от вирусов.

28. Условия (правила) безопасной работы компьютерных систем и технология обнаружения заражения вирусами.

29. Программно-аппаратные комплексы противодействия несанкционированному межсетевому доступу. Функции, схема подключения и структура межсетевого экрана.

30. Контроль целостности и системные вопросы защиты программ и данных на этапе эксплуатации компьютерных систем.

31. Программно-аппаратные комплексы противодействия несанкционированному межсетевому доступу. Типы межсетевых экранов, поясните действие экранирующего маршрутизатора.

32. Перечислите и поясните этапы построения системы информационно-компьютерной безопасности, недостатки которых могут использоваться для разработки атак.

33. Программно-аппаратные комплексы противодействия несанкционированному межсетевому доступу. Типы межсетевых экранов, поясните действие шлюза сеансового уровня.

34. Перечислите и поясните функции системы защиты информации, которые следует проанализировать при поиске уязвимостей компьютерных систем.

35. Программно-аппаратные комплексы противодействия несанкционированному межсетевому доступу. Типы межсетевых экранов, поясните действие прикладного шлюза.

36. Представьте классификацию VPN сети по уровням модели OSI (эталонной модели взаимодействия открытых систем (ЭМ ВОС)), дайте определение этим группам. Представьте классификацию VPN по архитектуре технического решения и по способу технической реализации.

37. Какие протоколы формирования защищенного канала относятся к канальному уровню модели OSI (эталонной модели взаимодействия открытых систем (ЭМ ВОС)). Представьте архитектуру протоколов PPTP и L2TP, поясните их

38. Перечислите и поясните протоколы формирования защищенного канала на сеансовом уровне модели OSI (эталонной модели взаимодействия открытых систем (ЭМ ВОС)).

39. . Поясните протокол формирования защищенного канала на сетевом уровне модели OSI (эталонной модели взаимодействия открытых систем (ЭМ ВОС)), представьте его архитектуру и поясните (какие протоколы в него входят, поясните их).

Приложение 3

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

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

МЕТОДИЧЕСКИЕ УКАЗАНИЯ
по дисциплине «Защита информационных процессов в компьютерных системах»
Направление подготовки 10.03.01 Информационная безопасность
профиль «Комплексная защита объектов информатизации»
Форма подготовки очная

Владивосток
2019

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Количество аудиторных часов, отведенных на изучение дисциплины «Защита информационных процессов в компьютерных системах», составляет 72 часа. На самостоятельную работу – 72 час. 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 экзамен. Самостоятельная работа при подготовке к экзамену включает изучение теоретического материала с использованием лекционных материалов, рекомендуемых источников и материалов лабораторных работ.

Методические указания для написания реферата

Прежде всего, нужно выбрать тему реферата и подобрать соответствующую литературу. После ознакомления с литературой следует приступить к составлению плана. План реферата должен состоять из названия (темы), введения, основной части, заключения и списка использованной литературы (3-5 работ). Основная часть, как правило, разбивается на дополнительные вопросы (не более 3-4).

Объём реферата должен быть не менее 12 машинописных страниц.

Во введении описывается цель, задачи работы, а также раскрываются смысл и значение основных понятий выбранной темы, область их применения.

В основной части необходимо:

г) ещё раз уточнить тему работы;

д) разбить основную часть работы на дополнительные вопросы;

е) дать ответы на эти вопросы, получив вспомогательные результаты. На их основе дать ответ на основной вопрос. Допускаются ссылки на дополнительную литературу.

В заключении подводятся итоги исследования. Заключение не должно быть большим по объёму.