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)
«Теория и проектирование защищенных систем»
Направление –10.03.01 «Информационная безопасность»
Профиль подготовки - «Комплексная защита объектов информатизации»
Форма подготовки – очная

курс 4 семестр 7
лекции 36 час.
практические занятия час.
лабораторные работы 72 час.
в том числе с использованием МАО лек. / пр. / лаб. час.
всего часов аудиторной нагрузки 108 час.
в том числе с использованием МАО час.
самостоятельная работа 72 час.
в том числе на подготовку к экзамену 36 час.
контрольные работы (количество) учебным планом не предусмотрены
курсовая работа / курсовой проект 7 семестр
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): Добржинский Ю.В., к.т.н., с.н.с.

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
«Теория и проектирование защищенных систем»

Дисциплина «Теория и проектирование защищенных систем» объединяет и систематизирует наиболее важные понятия в сфере создания и эксплуатации защищенных систем, раскрывает вопросы нормативно-методической регламентации функциональной структуры (архитектуры) подсистем безопасности защищенных компьютерных систем (КС), функциональные требования безопасности к продуктам и системам информационных технологий (ИТ), жизненный цикл, порядок создания и эксплуатации защищенных систем, продуктов и систем ИТ, удовлетворяющих требованиям информационной безопасности.

Общая трудоемкость освоения дисциплины составляет 216 часов (6 з.е.). Учебным планом предусмотрены лекционные занятия (36 час.), лабораторные работы (72 час.), самостоятельная работа студентов (72 час.), контроль качества обучения студентов (36 час.). Дисциплина реализуется на 4 курсе в 7 семестре. Форма контроля по дисциплине – экзамен.

Знания и практические навыки, полученные из дисциплины «Теория и проектирование защищенных систем», используются студентами при разработке курсовых и дипломных работ.

Цель: раскрыть нормативно-методическое регулирование процессов создания и эксплуатации защищенных автоматизированных систем, безопасных продуктов и систем информационных технологий. Дать студентам основы методов и технологий создания защищенных систем.

Задачи:

- дать основы стандартизации (нормативно-методической регламентации) требований к защищенным системам, процессов их создания и эксплуатации;
- дать основы методов и технологий проектирования защищенных систем;

- дать основы управления проектированием защищенных систем;

- дать основы практических навыков работы с нормативно методическими документами (стандартами), умений составления основных документов на этапах создания и эксплуатации защищенных систем.

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

Код и формулировка компетенции	**Этапы формирования компетенции**	
(ОК-4) способностью творчески воспринимать и использовать достижения науки, техники в профессиональной сфере в соответствии с потребностями регионального и мирового рынка труда	Знает	общие понятия формализованного описания процесса обработки данных, и различия между технологией программирования, программной инженерией и методологией программирований
	Умеет	определять требования к программному средству, включающие формулировку математической постановки предметной задачи и выбор метода ее решения, документально их закрепить их
	Владеет	необходимым инструментарием технологии программирования математического и информационного плана для анализа предметной области, обоснования и создания программных средств для насущных ее задач, ориентированных на автоматизацию процессов в различных сферах деятельности человека
(ПК-4) способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	Знает	принципы и методы организационной защиты информации
	Умеет	анализировать и оценивать степень риска проявления факторов опасности систем «Человек – среда обитания», осуществлять и контролировать выполнение требований по охране труда и технике безопасности в конкретной сфере деятельности
	Владеет	методами анализа и формализации информационных процессов объекта и связей между ними
(ПК-8) способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования	Знает	основы информационной безопасности
	Умеет	принимать участие в эксплуатации подсистем управления информационной безопасностью
	Владеет	навыками применения мер по защите информации

соответствующих проектных решений		
(ПК-9) способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	Знает	подсистемы информационной безопасности объекта
	Умеет	администрировать подсистемы информационной безопасности объекта
	Владеет	навыками администрирования

Для формирования вышеуказанных компетенций в рамках дисциплины «Теория и проектирование защищенных систем» применяются следующие методы обучения: чтение лекций/чтение лекций с использованием мультимедийного оборудования (проектор)/ проведение и сдача лабораторных работ. Используемые оценочные средства: лабораторные работы (ПР-6), конспект (ПР-7).

I. СТРУКТУРА И СОДЕРЖАНИЕ ТЕОРЕТИЧЕСКОЙ ЧАСТИ КУРСА

МОДУЛЬ 1. Основы теории информационной безопасности (18 час.)

Раздел I. Структура теории информационной безопасности (8 час.)

Тема 1. Основные понятия теории информационной безопасности (2 час.)

Основные термины и определения теории информационной безопасности. Что такое преобразование информации. Аксиома теории информационной безопасности.

Тема 2. Ценность информации (2 час.)

Чтобы защитить информацию, надо затратить силы и средства, а для этого надо знать какие потери мы могли бы понести. Ясно, что в денежном выражении затраты на защиту не должны превышать возможные потери. Для решения этих задач в информацию вводятся вспомогательные структуры - ценность информации.

Тема 3. Анализ угроз информационной безопасности (2 час.)

Свойства информации. Что такое угроза. Угроза конфиденциальности информации. Угроза целостности информации. Угроза отказа служб. Другие классификации угроз.

Тема 4. Структура теории информационной безопасности (2 час.)

Основные уровни защиты информации. Защита магнитных носителей информации.

Раздел II. Формальные политики безопасности (6 час.)

Тема 1. Понятие формальной политики безопасности (2 час.)

Интегральной характеристикой, описывающей свойства защищаемой системы, является политика безопасности - качественное (или качественно-количественное) описание свойств защищенности, выраженное в терминах, описывающих систему. Описание политики безопасности может включать или учитывать свойства злоумышленника и объекта атаки.

Тема 2. Основные типы формальных политик безопасности (2 час.)

Дискреционная политика безопасности. Мандатная политика безопасности.

Тема 3. Разработка и реализация формальных политик безопасности (2 час.)

Каким образом происходит реализация формальных политик безопасности. На какие критерии стоит опираться при разработке формальных политик безопасности.

Раздел III. Математические модели информационной безопасности (4 час.)

Тема 1. Классификация математических моделей информационной безопасности по основным видам угроз (2 час.)

Формальные модели необходимы и используются достаточно широко, потому что только с их помощью можно доказать безопасность системы опираясь при этом на объективные и неопровержимые постулаты математической теории. модели безопасности позволяют обосновать жизнеспособность системы и определяют базовые принципы ее архитектуры

и используемые при ее построении технологические решения Основная цель создания политики безопасности информационной системы и описания ее в виде формальной модели — это определение условий, которым должно подчиняться поведение системы, выработка критерия безопасности и проведение формального доказательства соответствия системы этому критерию при соблюдении установленных правил и ограничений.

Тема 2. Модели разграничения доступа (2 час.)

Подробное математическое описание некоторых математических моделей, таких как дискреционная модель ХРУ, модель Take-Grant, расширенная модель Take-Grant, мандатная модель Белла-ЛаПадулы и т.д.

МОДУЛЬ 2. Защищенные системы безопасности (18 час.)

Раздел I. Основные критерии защищенности АС. Классы защищенности (6 час.)

Тема 1. Стандарт оценки безопасности компьютерных систем TCSEC («Оранжевая книга») (2 час.)

«Оранжевая книга» предусматривает четыре группы критериев, которые соответствуют различной степени защищенности: от минимальной (группа D) до формально доказанной (группа A). Подробное рассмотрение всех этих групп.

Тема 2. Концепции защиты АС и СВТ по руководящим документам ФСТЭК РФ (2 час.)

Структура требований безопасности. Классы защищенности АС.

Тема 3. Критерии оценки безопасности информационных технологий (Common Criteria) (2 час.)

Основные понятия. Функциональные требования. Требования доверия безопасности.

Раздел II. Основные этапы построения защищенной информационной системы (8 час.)

Тема 1. Законодательный уровень (2 час.)

Закон РФ «Об информации, информатизации и защите информации», закон РФ «О лицензировании отдельных видов деятельности», пакет руководящих документов ФСТЭК, концепция защиты средств вычислительной техники и АС от НСД к информации и т.д.

Тема 2. Административный уровень (2 час.)

Политика безопасности, анализ рисков, анализ угроз, оценка рисков.

Тема 3. Процедурный уровень (2 час.)

Основные классы мер процедурного уровня: управление персоналом, физическая защита, поддержание работоспособности, реагирование на нарушение режимов безопасности, планирование восстановительных работ.

Тема 4. Программно-технический уровень (2 час.)

Последний уровень формирования защищенной информационной системы отвечает за выработку программно-технических мер и, соответственно, носит название программно-технического уровня.

Основные механизмы: идентификация и аутентификация, разграничение доступа, регистрация и аудит, криптография, экранирование.

Основные средства: средства контроля доступа, средства шифрования, средства антивирусной защиты и т.д.

Раздел III. Контроль безопасности информационной системы (4 час.)

Тема 1. Нормативная база аудита (2 час.)

Законодательство в области аудита безопасности, стандарты аудиторской деятельности.

Тема 2. Методы и средства аудита безопасности информационных систем (2 час.)

Активный аудит и его место среди других сервисов безопасности, виды аудита, влияние аудита безопасности на развитие компании, основные этапы проведения аудита, методика анализа защищенности и т.д.

I. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКОЙ ЧАСТИ КУРСА

Практические занятия (18 час.)

Занятие 1. Закрепление теоретических знаний по 1-му и 2-му разделам 1-го модуля. **(1.5 час.)**

Занятие 2. Математические модели информационной безопасности **(3 час.)**

Занятие 3. Стандарт оценки безопасности компьютерных систем TCSEC **(2 час.)**

Занятие 4. Классы защищенности систем. Руководящие документы ФСТЭК **(2 час.)**

Занятие 5. Основные этапы построения защищенной информационной системы. Законодательный и административный уровни **(3 час.)**

Занятие 6. Основные этапы построения защищенной информационной системы. Процедурный уровень **(1.5 час.)**

Занятие 7. Основные этапы построения защищенной информационной системы. Программно-технический уровень **(2.5 час.)**

Занятие 8. Контроль безопасности информационной системы **(2.5 час.)**

Лабораторные работы (72 час.)

Лабораторная работа №1. Математические модели информационной безопасности **(12 час.)**

Лабораторная работа №2. Подбор нормативно-правовой базы и руководящих документов, необходимых для построения защищенных систем **(12 час.)**

Лабораторная работа №3. Проектирование защищенной системы. Законодательный и административный уровни **(12 час.)**

Лабораторная работа №4. Проектирование защищенной системы процедурный уровень **(12 час.)**

Лабораторная работа №5. Проектирование защищенной системы. Программно-технический уровень **(12 час.)**

Лабораторная работа №6. Проектирование защищенной системы. Рассмотрение достоинств, недостатков и ошибок полученной системы**. (12 час.)**

III. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине «Теория и проектирование защищенных систем» 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. Основы теории информационной безопасности	ОПК-6, ПК-4, ПК-6, ПК-16, ПК-17	знает	ПР-1	1-16
			умеет	ПР-6	1-16
			владеет	ПР-7	1-16
2	МОДУЛЬ 2. Защищенные системы безопасности	ОПК-6, ПК-4, ПК-6, ПК-16, ПК-17	знает	ПР-7	17-29
			умеет	ПР-6	17-29
			владеет	ПР-5	17-29

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. Пакин А.И. Информационная безопасность информационных систем управления предприятием / А.И. Пакин – М. : Московская государственная академия водного транспорта, 2009. – 41 с. – Режим доступа: https://elibrary.ru/item.asp?id=27912493

2. Садердинов А.А., Трайнёв В.А., Федулов А.А. Информационная безопасность предприятия / А.А. Садердинов, В.А. Трайнёв, А.А. Федулов – М. : Дашков и Ко, 2004. – 335 с. – Режим доступа: https://elibrary.ru/item.asp?id=19749140

3. Галатенко В.А. Стандарты информационной безопасности – М: ИНТУИТ НОУ, 2016, 308с. http://lib.dvfu.ru:8080/lib/item?id=chamo:277429&theme=FEFU

4. Вавренюк В.Г. Операционные системы Windows : методические указания к лабораторным работам Windows Server 2008 Enterprise: учебно-методическое пособие. Владивосток: Изд-во Дальневосточного университета, 2010. – 110 с. - http://lib.dvfu.ru:8080/lib/item?id=chamo:292830&theme=FEFU

Дополнительная литература

(печатные и электронные издания)

1. Шелупанов А. А. Основы защиты информации / А.А. Шелупанов – Томск : В-Спектр, 2007. – 185 с. – Режим доступа: https://elibrary.ru/item.asp?id=19590228

2. Белим С.В. Защита в операционных системах / С.В. Белим – Омск : Изд-во Омского гос. ун-та, 2011. – 51 с. – Режим доступа: https://elibrary.ru/item.asp?id=19597414Эндрю

3. Таненбаум, Переводчики: Н. Вильчинский, Андрей Лашкевич, / Современные операционные системы (ModernOperatingSystems) / Издательский дом «Питер», 2013, 1120с. http://lib.dvfu.ru:8080/lib/item?id=chamo:784076&theme=FEFU

4. Борисенко М.Л., Дудоров Е.Н., Корольков Ю.Д. Защита информации в операционных системах MS Windows / М.Л. Борисенко, Е.Н. Дудоров, Ю.Д. Корольков – Иркутск : Иркутский государственный университет, 2012. – 120 с. – Режим доступа: https://elibrary.ru/item.asp?id=23986125

5. Варлатая С.К., Шаханова М.В. Защита информационных процессов в компьютерных сетях : учебно-методический комплекс для вузов - Владивосток : Изд-во Дальневосточного технического университета, 2008. – 216 с. - http://lib.dvfu.ru:8080/lib/item?id=chamo:384163&theme=FEFU

Интернет-ресурсы

1. Встраиваемые системы на основе Linux. Издательство "ДМК Пресс". 2017, 360 страниц.
2. http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=4925 - Пушкарев В.В. «Защита информационных процессов в компьютерных

системах», Издательство: ТУСУР (Томский государственный университет систем управления и радиоэлектроники), Год: 2012, 131 стр.

3. http://window.edu.ru/resource/836/69836 - Марапулец Ю.В. Операционные системы: Учебное пособие для студентов специальности 230105 "Программное обеспечение вычислительной техники и автоматизированных систем" очной формы обучения. - Петропавловск-Камчатский: КамчатГТУ, 2008. - 235 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 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

Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 314, Специализированная лаборатория кафедры ИБ. 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 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 «Теория и проектирование защищенных систем», составляет 126 часов. На самостоятельную работу – 54 часа. При этом аудиторная нагрузка состоит из 36 лекционных часов, 72 часов лабораторных работ и 18 часов практических занятий.

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

Подготовка к практическим занятиям и лабораторным работам предполагает повторение лекционного материала. В результате студент должен быть готов к выполнению заданий на практическом занятии и выполнению лабораторных работ. Основой практической составляющей является выполнение одного практического задания с последующим

предоставлением отчета о выполнении. Основой 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 по практическим занятиям и 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 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
Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 314, Специализированная лаборатория кафедры ИБ. 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 – 15) Оборудование: "Компьютер DNS Office (автоматизированное рабочее место), Рабочее место сотрудников в составе: системный блок, клавиатура, мышь, монитор 17"" Aser-173 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 «Теория и проектирование защищенных систем»
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	Работа с конспектом, изучение литературы по дисциплине, подготовка к практическому занятию, выполнение лабораторных работ	27	ПР-1, ПР-4, ПР-6
2	Сессия	Подготовка к экзамену	27	Экзамен

Рекомендации по самостоятельной работе студентов

Самостоятельная работа по курсу «Теория и проектирование защищенных систем» предусматривает три основных вида самостоятельной работы: подготовку к практическим занятиям, тестам и выполнение лабораторных работ.

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 и материалов по практическим занятиям.

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 «Теория и проектирование защищенных систем»
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 применять приемы оказания первой помощи, методы и средства защиты персонала предприятия и населения в условиях чрезвычайных ситуаций, организовать мероприятия по охране труда и технике безопасности (ОПК-6);	Знает	Опасные и вредные факторы системы «человек-среда обитания», методы анализа антропогенных опасностей, научные и организационные основы защиты окружающей среды и ликвидации последствий аварий, катастроф, стихийных бедствий
	Умеет	Анализировать и оценивать степень риска проявления факторов опасности системы «человек-среда обитания», осуществлять и контролировать выполнение требований по охране труда и технике безопасности в конкретной сфере деятельности
	Владеет	Навыками безопасного использования технических средств в профессиональной деятельности
способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты (ПК-4);	Знает	Принципы и методы организационной защиты информации
	Умеет	Анализировать и оценивать степень риска проявления факторов опасности систем «Человек – среда обитания», осуществлять и контролировать выполнение требований по охране труда и технике безопасности в конкретной сфере деятельности
	Владеет	Методами анализа и формализации информационных процессов объекта и связей между ними
способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации (ПК-6);	Знает	Принципы и методы организационной защиты информации, а так же основные нормативные правовые акты в области информационной безопасности и защиты информации
	Умеет	Анализировать и оценивать угрозы информационной безопасности объекта
	Владеет	Методами анализа и формализации информационных процессов объекта и связей между ними и профессиональной терминологией
способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной	Знает	Правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны
	Умеет	Анализировать и оценивать угрозы информационной безопасности объекта

безопасности, управлять процессом их реализации (ПК-16);	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. Основы теории информационной безопасности	ОПК-6, ПК-4, ПК-6, ПК-16, ПК-17	знает	ПР-1	1-16
			умеет	ПР-6	1-16
			владеет	ПР-7	1-16
2	МОДУЛЬ 2. Защищенные системы безопасности	ОПК-6, ПК-4, ПК-6, ПК-16, ПК-17	знает	ПР-7	17-29
			умеет	ПР-6	17-29
			владеет	ПР-5	17-29

Оценочные средства для промежуточной аттестации
Список вопросов на экзамен

1. Информационные системы. Общие сведения.
2. Автоматизированная информационная система.
3. Принципы внедрения и функционирования АИС. Основные определения.
4. Классификация ИС и АИС.

5. Четыре типа АИС с точки зрения выполняемых ими процессов.

6. Состав АИС.

7. Проектирование ИС и АИС. Основные определения.

8. Моделирование разработки АИС. Основные определения.

9. Основные особенности жизненного цикла АИС.

10. Последовательность проектирования АИС.

11. Планирование работ.

12. Методы проектирования АИС. Основные определения.

13. Средства проектирования АИС.

14. Программная инженерия и CASE-средства. Основные определения.

15. Этапы проектирования АИС.

16. Паспортизация объектов и систем.

17. Разработка Технического задания на создание АИС.

18. Стадии и этапы проектирования АИС.

19. ГОСТы, используемые для проектирования автоматизированных информационных систем.

20. Предпроектное исследование. Общие положения.

21. Анализ системы.

22. Техническое задание на АИС.

23. Правила оформления ТЗ на создание АИС.

24. Состав и содержание Технического задания.

25. Требования по безопасности, по сохранности информации, к видам обеспечения, к документированию и др.

26. Источники разработки системы, порядок контроля и приемки системы.

27. Основные правила оформления ТЗ на АИС.

28. Дополнительные рекомендации по разработке ТЗ на программно-технические комплексы и их составляющие.

29. Реально сложившаяся практика проектирования АИС.

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 «Теория и проектирование защищенных систем»
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 «Теория и проектирование защищенных систем», составляет 126 часов. На самостоятельную работу – 54 часа. При этом аудиторная нагрузка состоит из 36 лекционных часов, 72 часов лабораторных работ и 18 часов практических занятий.

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

Подготовка к практическим занятиям и лабораторным работам предполагает повторение лекционного материала. В результате студент должен быть готов к выполнению заданий на практическом занятии и выполнению лабораторных работ. Основной практической составляющей является выполнение одного практического задания с последующим предоставлением отчета о выполнении. 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 по практическим занятиям и лабораторных работ.