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

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

«СОГЛАСОВАНО»
Руководитель ОП

_____ Добржинский Ю.В
(подпись) (Ф.И.О.)

«УТВЕРЖДАЮ»
И.о. заведующего кафедрой
информационной безопасности

_____ Добржинский Ю.В
(подпись) (Ф.И.О.)

« 15 » июня 2019 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Модели безопасности компьютерных систем
Специальность 10.05.01 Компьютерная безопасность
(Математические методы защиты информации)
Форма подготовки очная

курс 5 семестр 9
лекции 36 час.
практические занятия 18 час.
лабораторные работы 00 час.
в том числе с использованием МАО лек. 9 / пр. 00 / лаб. 00 час.
в том числе в электронной форме лек. 00 / пр. 00 / лаб. 00 час.
всего часов аудиторной нагрузки 54 час.
в том числе с использованием МАО 9 час.
в том числе в электронной форме 00 час.
самостоятельная работа 54 час.
в том числе на подготовку к экзамену 27 час.
курсовая работа / курсовой проект не предусмотрены
зачет не предусмотрен
экзамен 9 семестр

Рабочая программа составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования, утвержденного приказом Министерства образования и науки РФ от 01.12.2016 № 1512

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

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

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)

ABSTRACT

Specialist's degree in 10.05.01 Computer Security
Specialization "Mathematical Methods for Information Security"
Course title: *Computer systems security models*
Basic part of Block , _3_credits
Instructor: *Dobrzhinsky Yu.V.*

At the beginning of the course a student should be able to:

• ability to correctly apply the apparatus of mathematical analysis, geometry, algebra, discrete mathematics, mathematical logic, theory of algorithms, probability theory, mathematical statistics, information theory, number-theoretic methods (OPK-2) when solving professional problems;
• the ability to understand the importance of information in the development of modern society, to apply the achievements of information technologies to search and process information on the profile of activities in global computer networks, library collections and other sources of information (OPK-3);
• ability to apply research methods in professional activities, including in the work on interdisciplinary and innovative projects (OPK-4);
• ability to use programming languages and systems, tools for solving professional, research and applied tasks (OPK-8).

Learning outcomes:

(OPK-7) the ability to take into account modern trends in the development of computer science and computer technology, computer technology in their professional activities, to work with software tools for general and special purposes
(OPK-9) the ability to develop formal models of security policies, access control policies and information flows in computer systems, taking into account information security threats
(PC-4) the ability to analyze and participate in the development of mathematical models of computer systems security

Course description:

Discipline has a theoretical focus, with great importance for the development of discipline, as lecture and practical classes. During the implementation of the discipline in the framework of lectures and practical exercises, active / interactive learning methods are used that implement a visual representation of the results of the analysis of models. This discipline covers such issues as the classification of modern computer systems, basic concepts of mathematical logic and theory of algorithms, sources and classification of information security threats, basic tools and methods for ensuring information security, principles for constructing information protection systems, protective mechanisms and means of ensuring the security of operating systems.

Main course literature:

1. Ю. В. Доброжинский / Диагностика компьютерных систем : учебно-методический комплекс. Владивосток : Изд-во Дальневосточного

технического университета, 2008. – 113 с. - http://lib.dvfu.ru:8080/lib/item?id=chamo:383420&theme=FEFU

2. Верещагина Е.А. Корпоративные информационные системы : учебно-методический комплекс. Владивосток : Изд-во Дальневосточного технического университета, 2008. – 103 с. - http://lib.dvfu.ru:8080/lib/item?id=chamo:384662&copies-page=1&theme=FEFU

3. Безопасность и управление доступом в информационных системах: Учебное пособие / А.В. Васильков, И.А. Васильков. - М.: Форум: НИЦ ИНФРА-М, 2013. - 368 с.: ил.; 60x90 1/16. - (Профессиональное образование). (переплет) ISBN 978-5-91134-360-6 - Режим доступа: http://znanium.com/catalog/product/405313

4. Альпидовский, А.Д. Компьютерные системы и сети [Электронный ресурс] : учебное пособие / А.Д. Альпидовский. — Электрон. дан. — Нижний Новгород : ВГУВТ, 2012. — 156 с. — Режим доступа: https://e.lanbook.com/book/60800

5. Комплексное обеспечение информационной безопасности автоматизированных систем [Электронный ресурс]: лабораторный практикум/ М.А. Лапина [и др.].— Электрон. текстовые данные.— Ставрополь: Северо-Кавказский федеральный университет, 2016.— 242 c.— Режим доступа: http://www.iprbookshop.ru/62945.html

Form of final control: *exam*

Аннотация к рабочей программе дисциплины
«Модели безопасности компьютерных систем»

Рабочая программа учебной дисциплины «Модели безопасности компьютерных систем» разработана для студентов, обучающихся по специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит в базовую часть учебного плана с кодом Б1.Б.26.

Общая трудоемкость дисциплины «Модели безопасности компьютерных систем» составляет 3 зачетных единицы – 108 академических часа. Среди них на лекции выделено 36 часов, практические занятия 18 часов, на самостоятельную работу 54 часа, среди них на подготовку к экзамену 27 часов. Дисциплина реализуется на 5 курсе в 9 семестре. Форма контроля по дисциплине – экзамен.

Дисциплина «Модели безопасности компьютерных систем» основана на предварительном изучении следующих дисциплин: «Информатика», «Математическая логика и теория алгоритмов», «Дискретная математика», «Основы информационной безопасности». Знания и практические навыки, полученные при изучении дисциплины «Модели безопасности компьютерных систем», обеспечивают освоение следующих дисциплин:

«Защита в операционных системах», «Основы построения защищенных компьютерных сетей», «Основы построения защищенных баз данных», «Программно-аппаратные средства обеспечения информационной безопасности», «Надежность программного обеспечения».

Дисциплина имеет теоретическую направленность, при этом большое значение для освоения дисциплины имеют, как лекционные, так и практические занятия. В ходе реализации дисциплины в рамках лекционных и практических занятий применяются методы активного/ интерактивного обучения, реализующие наглядное представление результатов анализа моделей. Данная дисциплина затрагивает такие вопросы, как классификация современных компьютерных систем, основные понятия математической логики и теории алгоритмов, источники и классификация угроз информационной безопасности, основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации, защитные механизмы и средства обеспечения безопасности операционных систем.

Цель курса – обучение специалистов принципам построения формальных моделей политик безопасности, политик управления доступом и информационными потоками, методам анализа математических моделей защищаемых систем и систем обеспечения информационной безопасности КС.

Задачи:

- изучение основных угроз безопасности информации и модели нарушителя в КС.
- изучить основные виды политик управления доступом и информационными потоками в КС.
- изучить основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков.
- научить разрабатывать модели угроз и модели нарушителя безопасности КС.

- научить разрабатывать частные политики безопасности КС, в том числе политики управления доступом и информационными потоками.

Для успешного изучения дисциплины «Модели безопасности компьютерных систем» у обучающихся должны быть сформированы следующие предварительные компетенции:

- способность корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов (ОПК-2);
- способность понимать значение информации в развитии современного общества, применять достижения информационных технологий для поиска и обработки информации по профилю деятельности в глобальных компьютерных сетях, библиотечных фондах и иных источниках информации (ОПК-3);
- способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ОПК-4);
- способность использовать языки и системы программирования, инструментальные средства для решения профессиональных, исследовательских и прикладных задач (ОПК-8).

В результате изучения дисциплины у обучающихся формируются следующие общепрофессиональные и профессиональные компетенции.

Код и формулировка компетенции	**Этапы формирования компетенции**	
(ОПК-7) способность учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специального	Знает	основные виды политик управления доступом и информационными потоками в компьютерных системах; основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков.
	Умеет	осуществлять подбор, изучение и

назначения		обобщение научно-технической информации, нормативных и методических материалов по методам обеспечения информационной безопасности компьютерных систем.
	Владеет	навыком формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем
(ОПК-9) способность разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации	Знает	основные виды политик управления доступом и информационными потоками в компьютерных системах; основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков.
	Умеет	использовать основные виды политик управления доступом и информационными потоками в компьютерных системах; использовать основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков.
	Владеет	методами разработки частных политик безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками.
(ПК-4) способность проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем	Знает	математические основы моделей безопасности; основы постановки научной задачи, определения гипотезы и методов исследования безопасности компьютерных систем
	Умеет	построить формальную модель системы, соответствующую заданной политике безопасности; научно и теоретически обосновано излагать результаты исследований безопасности компьютерных систем
	Владеет	методами анализа безопасности компьютерных систем с использованием формальных моделей безопасности; методиками исследований в области безопасности компьютерных систем

Для формирования вышеуказанных компетенций в рамках дисциплины «Модели безопасности компьютерных систем» применяются следующие методы активного/ интерактивного обучения: интерактивные и проблемные

лекции, лекции-диалоги, работа в малых группах, метод обучения в парах. Используемые оценочные средства: конспект (ПР-7), собеседование (ОУ-1), коллоквиум (ОУ-2).

I. СТРУКТУРА И СОДЕРЖАНИЕ ТЕОРЕТИЧЕСКОЙ ЧАСТИ КУРСА

Лекционные занятия (36 час.)

Раздел I. Основные понятия и определения, используемые при описании моделей безопасности компьютерных систем (4 час.)

Тема 1. Элементы теории компьютерной безопасности (2 час.)

1.1. Сущность, субъект, доступ, информационный поток.

1.2. Ценность информации: аддитивная модель, порядковая шкала ценности, решетка ценности.

Тема 2. Угрозы безопасности и уровни защиты информации (1 час.)

2.1. Классическая классификация угроз безопасности информации. Виды информационных потоков.

2.2. Уровни защиты информации. Основные виды атак на автоматизированные системы и методы защиты в зависимости от вида угрозы и уровня защиты информации.

Тема 3. Классификация и проблемы применения моделей безопасности (1 час.)

3.1. Виды политик управления доступом и информационными потоками: дискреционная политика управления доступом, мандатная политика управления доступом, политика ролевого управления доступом, политика безопасности информационных потоков, политика изолированной программной среды.

3.2. Основные виды формальных моделей безопасности. Проблемы реализации модели безопасности.

Раздел II. Модели компьютерных систем с дискреционным управлением доступом (12 час.)

Тема 1. Модель матрицы доступов Харрисона-Руззо-Ульмана (4 час.)

1.1. Описание модели.

1.2. Анализ безопасности систем ХРУ.

1.3. Модель типизированной матрицы доступов.

Тема 2. Модель распространения прав доступа Take-Grant (4 час.)

2.1. Основные положения классической модели Take-Grant.

2.2. Расширенная модель Take-Grant.

2.3. Представление систем Take-Grant системами ХРУ.

Тема 3. Дискреционные ДП-модели (4 час.)

3.1. Базовая ДП-модель.

3.2. ДП-модель без кооперации доверенных и недоверенных субъектов.

Раздел III. Модели изолированной программной среды (6 час.)

Тема 1. Субъектно-ориентированная модель изолированной программной среды (2 час.)

1.1. Понятие и структура изолированной программной среды.

Тема 2. Корректность субъектов в ДП-моделях КС с дискреционным управлением доступом (4 час.)

2.1. ДП-модель с функционально ассоциированными с субъектами сущностями.

2.2. ДП-модель с функционально или параметрически ассоциированными с субъектами сущностями.

2.3. Применение ФАС ДП-модели для анализа безопасности веб-систем.

Раздел IV. Модели компьютерных систем с мандатным управлением доступом (6 час.)

Тема 1. Модель Белла-ЛаПадулы (4 час.)

1.1. Классическая модель Белла-ЛаПадулы.

1.2. Пример некорректного определения свойств безопасности.

1.3. Политика low-watermark в модели Белла-ЛаПадулы.

1.4. Примеры реализации запрещенных информационных потоков.

1.5. Безопасность переходов.

1.6. Модель мандатной политики целостности информации Биба.

Тема 2. Модель систем военных сообщений (2 час.)

2.1. Общие положения и основные понятия.

2.2. Неформальное описание модели СВС.

2.3. Формальное описание модели СВС.

Раздел V. Модели безопасности информационных потоков (3 час.)

Тема 1. Автоматная модель безопасности информационных потоков (1 час.)

1.1. Автоматная модель безопасности информационных потоков

Тема 2. Программная модель контроля информационных потоков (1 час.)

2.1. Программная модель контроля информационных потоков

Тема 3. Вероятностная модель безопасности информационных потоков (1 час.)

3.1. Вероятностная модель безопасности информационных потоков

Раздел VI. Модели компьютерных систем с ролевым управлением доступом (5 час.)

Тема 1. Понятие ролевого управления доступом и базовая модель ролевого управления доступом (1 час.)

1.1. Понятие ролевого управления доступом и базовая модель ролевого управления доступом

Тема 2. Модель администрирования ролевого управления доступом (2 час.)

2.1. Основные положения.

2.2. Администрирование множеств авторизованных ролей пользователей.

2.3. Администрирование множеств прав доступа, которыми обладает роли.

2.4. Администрирование иерархии ролей.

Тема 3. Модель мандатного ролевого управления доступом (2 час.)

3.1. Защита от угрозы конфиденциальности информации.

3.2. Защита от угроз конфиденциальности и целостности информации .

II. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКОЙ ЧАСТИ КУРСА

Практические занятия (18 час.)

Занятие 1. Модель решетки. Модели ХРУ и ТМД (2 час.)

1. Описание модели
2. Анализ безопасности систем ХРУ
3. Модель типизированной матрицы доступов .

Занятие 2. Классическая модель Take-Grant (2 час.)

1. Основные положения классической модели Take-Grant

Занятие 3. Расширенная модель Take-Grant (2 час.)

1. Расширенная модель Take-Grant
2. Представление систем Take-Grant системами ХРУ

Занятие 4. Классическая модель Белла-ЛаПадулы и ее интерпретации (2 час.)

1. Классическая модель Белла-ЛаПадулы

2. Пример некорректного определения свойств безопасности
3. Политика Low-Watermark в модели Белла-ЛаПадулы

Занятие 5. Модель СВС (2 час.)

1. Общие положения и основные понятия
2. Неформальное описание модели СВС
3. Формальное описание модели СВС

Занятие 6. Модели безопасности информационных потоков (2 час.)

1. Автоматная модель безопасности информационных потоков
2. Программная модель контроля информационных потоков
3. Вероятностная модель безопасности информационных потоков

Занятие 7. Модели ролевого управления доступом (2 час.)

1. Понятие ролевого управления доступом
2. Базовая модель ролевого управления доступом
3. Модель администрирования ролевого управления доступом

Занятие 8. Дискреционные ДП-модели (2 час.)

1. ДП-модель с функционально ассоциированными с субъектами сущностями
2. ДП-модель для политики безопасного администрирования
3. ДП-модель для политики абсолютного разделения административных и пользовательских полномочи

Занятие 9. Мандатные и ролевые ДП-модели (2 час.)

1. Мандатная ДП-модель с блокирующими доступами доверенных субъектов
2. Мандатная ДП-модель с отождествлением порожденных субъектов
3. Мандатная ДП-модель КС, реализующих политику строгого мандатного управления доступом

III. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине «Модели безопасности компьютерных 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;

критерии оценки выполнения самостоятельной работы.

IV. КОНТРОЛЬ ДОСТИЖЕНИЯ ЦЕЛЕЙ КУРСА

№ п/п	Контролируемые разделы / темы дисциплины	Коды и этапы формирования компетенций		Оценочные средства	
				текущий контроль	промежуточная аттестация
1	Раздел I. Основные понятия и определения, используемые при описании моделей безопасности компьютерных систем	ОПК-7 ОПК-9 ПК-4	знает	конспект (ПР-7)	1-9
			умеет	собеседование (ОУ-1)	1-9
			владеет	коллоквиум (ОУ-2)	1-9
2	Раздел II. Модели компьютерных систем с дискреционным управлением доступом	ОПК-7 ОПК-9 ПК-4	знает	конспект (ПР-7)	10-13
			умеет	собеседование (ОУ-1)	10-13
			владеет	коллоквиум (ОУ-2)	10-13
3	Раздел III. Модели изолированной программной среды	ОПК-7 ОПК-9 ПК-4	знает	конспект (ПР-7)	14-16
			умеет	собеседование (ОУ-1)	14-16
			владеет	коллоквиум (ОУ-2)	14-16
4	Раздел IV. Модели компьютерных систем с мандатным управлением доступом	ОПК-7 ОПК-9 ПК-4	знает	конспект (ПР-7)	17-21
			умеет	собеседование (ОУ-1)	17-21
			владеет	коллоквиум (ОУ-2)	17-21
5	Раздел V. Модели безопасности информационных	ОПК-7 ОПК-9 ПК-4	знает	конспект (ПР-7)	22-24
			умеет		22-24

	потоков			собеседование (ОУ-1)	
			владеет	коллоквиум (ОУ-2)	22-24
6	Раздел VI. Модели компьютерных систем с ролевым управлением доступом	ОПК-7 ОПК-9 ПК-4	знает	конспект (ПР-7)	25-27
			умеет	собеседование (ОУ-1)	25-27
			владеет	коллоквиум (ОУ-2)	22-27

Типовые контрольные задания, методические материалы, определяющие процедуры оценивания знаний, умений и навыков и (или) опыта деятельности, а также критерии и показатели, необходимые для оценки знаний, умений, навыков и характеризующие этапы формирования компетенций в процессе освоения образовательной программы, представлены в Приложении 2.

Рейтинг-план по дисциплине «Модели безопасности компьютерных систем» на основании выполнении которого проводится текущая и промежуточная аттестация представлен в Приложении 3.

V. СПИСОК УЧЕБНОЙ ЛИТЕРАТУРЫ И ИНФОРМАЦИОННО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература

(электронные и печатные издания)

1. Ю. В. Добржинский / Диагностика компьютерных систем : учебно-методический комплекс. Владивосток : Изд-во Дальневосточного технического университета, 2008. – 113 с. - http://lib.dvfu.ru:8080/lib/item?id=chamo:383420&theme=FEFU

2. Верещагина Е.А. Корпоративные информационные системы : учебно-методический комплекс. Владивосток : Изд-во Дальневосточного технического университета, 2008. – 103 с. - http://lib.dvfu.ru:8080/lib/item?id=chamo:384662&copies-page=1&theme=FEFU

3. Безопасность и управление доступом в информационных системах: Учебное пособие / А.В. Васильков, И.А. Васильков. - М.: Форум: НИЦ ИНФРА-М, 2013. - 368 с.: ил.; 60x90 1/16. - (Профессиональное образование). (переплет) ISBN 978-5-91134-360-6 - Режим доступа: http://znanium.com/catalog/product/405313

4. Альпидовский, А.Д. Компьютерные системы и сети [Электронный ресурс] : учебное пособие / А.Д. Альпидовский. — Электрон. дан. — Нижний Новгород : ВГУВТ, 2012. — 156 с. — Режим доступа: https://e.lanbook.com/book/60800

5. Комплексное обеспечение информационной безопасности автоматизированных систем [Электронный ресурс]: лабораторный практикум/ М.А. Лапина [и др.].— Электрон. текстовые данные.— Ставрополь: Северо-Кавказский федеральный университет, 2016.— 242 с.— Режим доступа: http://www.iprbookshop.ru/62945.html

Дополнительная литература

(печатные и электронные издания)

1. Е.А. Дубинин. Оценка относительного ущерба безопасности информационной системы: Монография / Е.А. Дубинин, Ф.Б. Тебуева, В.В. Копытов. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2014. - 192 с. — Режим доступа: http://znanium.com/catalog/product/471787

2. Петров, А.А. Компьютерная безопасность. Криптографические методы защиты [Электронный ресурс] / А.А. Петров. — Электрон. дан. — Москва : ДМК Пресс, 2008. — 448 с. — Режим доступа: https://e.lanbook.com/book/3027

3. Кузнецов, О.П. Дискретная математика для инженера [Электронный ресурс] : учебное пособие / О.П. Кузнецов. — Электрон. дан. — Санкт-Петербург : Лань, 2009. — 400 с. — Режим доступа: https://e.lanbook.com/book/220

Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. Лекция 11: Основные направления обеспечения информационной безопасности компьютерных сетей учебных заведений [Электронный ресурс]. – Электрон. дан. – Режим доступа: https://tech.wikireading.ru/13010
2. Лекция 1: Безопасность компьютерных систем [Электронный ресурс]. – Электрон. дан. – Режим доступа: http://informaticslib.ru/news/item/f00/s06/n0000695/index.shtml
3. Лекция 4.2.: Модели безопасности и их применение [Электронный ресурс]. – Электрон. дан. – Режим доступа: http://wm-help.net/lib/b/book/4177904444/19

Перечень информационных технологий и программного обеспечения

Для работы в литературой из списка необходимо наличие к студента аккаунтов в указанных электронно-библиотечных системах: «Лань» (https://e.lanbook.com), «Знаниум» (http://znanium.com)

VI. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Количество аудиторных часов, отведенных на изучение дисциплины «Модели безопасности компьютерных систем», составляет 54 часа. На самостоятельную работу – 63 часа. При этом аудиторная нагрузка состоит из 36 лекционных часов и 18 часов практических занятий.

Обучающийся получает теоретические знания на лекционных занятиях, необходимые для последующего выполнения практических заданий. В ходе подготовки к лекциям должны использоваться источники из списка учебной литературы.

Студенту рекомендуется предварительно готовиться к лекции, используя ресурсы из списка, приведённого в разделе V, для более качественного освоения теоретического материала, а также возможности задать вопросы преподавателю.

При подготовке к практическим занятиям также необходимо повторить теоретический материал. Практические занятия представляют собой задания различного типа, направленные на получение обучающимся практических знаний по теме. В результате выполнения работы студент предоставляет преподавателю отчёт о проделанной работе, содержащий следующие пункты: цель работы, краткий теоретический материал, задание, ход работы,

результаты и выводы о проделанной работе.

Промежуточная форма аттестации - экзамен. Вопросы к экзамену соответствуют темам, изучаемым на лекционных занятиях. Таким образом, при самостоятельной подготовке к экзамену студенту необходимо воспользоваться конспектами лекций, а также иными источниками из списка литературы для более глубокого понимания материала.

VII. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 820, 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 – 19) Оборудование: "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, переносной компьютер (ноутбук Lenovo) с сумкой – 1 шт.

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 «Модели безопасности компьютерных систем»
Направление подготовки 10.05.01 Компьютерная безопасность
специализация «Математические методы защиты информации»
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 практического задания (выполнение отчета к занятию)	27	Отчет о выполнении практического задания
2	Сессия	Подготовка и сдача экзамена	27	Экзамен

Рекомендации по самостоятельной работе студентов

При подготовке отчета о выполнении практического задания должны использоваться источники из списка учебной литературы, а также примеры, рассмотренные на лекционных и практических занятиях. Отчет должен содержать:

- титульный лист;
- содержание;
- описание задания;
- решение;
- выводы.

Методические указания к выполнению отчета по занятию

Для получения **«зачтено»** отчет должен содержать основные пункты: титульный лист, содержание, описание задания, решение, выводы. При представлении отчета к сдаче обучающийся последовательно излагает принцип выполненной работы.

Оценка **«незачтено»** выставляется в случае, если отчет не содержит решения или выводов; обучающийся не может объяснить решение, излагает материал непоследовательно, сбивчиво.

Подготовка к практическим занятиям предполагает повторение лекционного материала и рассмотрение задач из раздела 2 РПУД. В результате студент должен быть готов на практическом занятии представить решение обозначенных задач. На практическом занятии студент обязан представить решение индивидуальной задачи. Рекомендуется представление решения задачи в виде презентации.

Оценка по результатам выполнения индивидуальных заданий осуществляется по следующим критериям: критичность и количество допущенных ошибок, самостоятельность выполнения задания, понимание основ по тематике задания, смысловой цельностью и последовательностью

изложения, демонстрация знаний и владения навыками самостоятельной работы по теме задания.

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 «Модели безопасности компьютерных систем»
Направление подготовки 10.05.01 Компьютерная безопасность
специализация «Математические методы защиты информации»
Форма подготовки очная

Владивосток
2019

Паспорт ФОС

Код и формулировка компетенции	Этапы формирования компетенции	
(ОПК-7) способностью учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специального назначения	Знает	Основные виды политик управления доступом и информационными потоками в компьютерных системах. Основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков.
	Умеет	Осуществлять подбор, изучение и обобщение научно-технической информации, нормативных и методических материалов по методам обеспечения информационной безопасности компьютерных систем.
	Владеет	Навыком формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем
(ОПК-9) способностью разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации	Знает	Основные виды политик управления доступом и информационными потоками в компьютерных системах. Основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков.
	Умеет	Использовать основные виды политик управления доступом и информационными потоками в компьютерных системах. Использовать основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков.
	Владеет	Методами разработки частных политик безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками.
(ПК-4) способностью проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем	Знает	Математические основы моделей безопасности. Основы постановки научной задачи, определения гипотезы и методов исследования безопасности компьютерных систем
	Умеет	Построить формальную модель системы, соответствующую заданной политике безопасности. Научно и теоретически

		обосновано излагать результаты исследований безопасности компьютерных систем
	Владеет	Методами анализа безопасности компьютерных систем с использованием формальных моделей безопасности. Методиками исследований в области безопасности компьютерных систем

№ п/п	Контролируемые разделы / темы дисциплины	Коды и этапы формирования компетенций		Оценочные средства	
				текущий контроль	промежуточная аттестация
1	Раздел I. Основные понятия и определения, используемые при описании моделей безопасности компьютерных систем	ОПК-7 ОПК-9 ПК-4	знает	конспект (ПР-7)	1-9
			умеет	собеседование (ОУ-1)	1-9
			владеет	коллоквиум (ОУ-2)	1-9
2	Раздел II. Модели компьютерных систем с дискреционным управлением доступом	ОПК-7 ОПК-9 ПК-4	знает	конспект (ПР-7)	10-13
			умеет	собеседование (ОУ-1)	10-13
			владеет	коллоквиум (ОУ-2)	10-13
3	Раздел III. Модели изолированной программной среды	ОПК-7 ОПК-9 ПК-4	знает	конспект (ПР-7)	14-16
			умеет	собеседование (ОУ-1)	14-16
			владеет	коллоквиум (ОУ-2)	14-16
4	Раздел IV. Модели компьютерных систем с мандатным управлением доступом	ОПК-7 ОПК-9 ПК-4	знает	конспект (ПР-7)	17-21
			умеет	собеседование (ОУ-1)	17-21
			владеет	коллоквиум (ОУ-2)	17-21
5	Раздел V. Модели	ОПК-7	знает	конспект	22-24

	безопасности информационных потоков	ОПК-9 ПК-4		(ПР-7)	
			умеет	собеседование (ОУ-1)	22-24
			владеет	коллоквиум (ОУ-2)	22-24
6	Раздел VI. Модели компьютерных систем с ролевым управлением доступом	ОПК-7 ОПК-9 ПК-4	знает	конспект (ПР-7)	25-27
			умеет	собеседование (ОУ-1)	25-27
			владеет	коллоквиум (ОУ-2)	22-27

Оценочные средства для промежуточной аттестации
Список вопросов на экзамен

1. Основные понятия теории компьютерной безопасности. Сущность, субъект, доступ, информационный поток. Задача защиты информации.
2. Ценность информации. Аддитивная модель. Анализ риска в рамках аддитивной модели.
3. Порядковая шкала ценностей. Модель решетки ценностей. MLS решетка.
4. Классическая классификация угроз безопасности информации. Виды информационных потоков.
5. Уровни защиты. Виды атак и методы защиты.
6. Виды политик управления доступом и информационными потоками.
7. Основные виды формальных моделей безопасности. Проблемы реализации модели безопасности.
8. Описание модели ХРУ. Анализ безопасности систем ХРУ.
9. Модель типизированной матрицы доступов.
10. Основные положения классической модели Take-Grant.
11. Расширенная модель Take-Grant. Представление систем Take-Grant системами ХРУ.
12. Базовая ДП-модель.
13. ДП-модель без кооперации доверенных и недоверенных субъектов.
14. Понятие и структура изолированной программной среды.
15. ДП-модель с функционально ассоциированными с субъектами сущностями.

16. ДП-модель с функционально или параметрически ассоциированными с субъектами сущностями.
17. Классическая модель Белла-ЛаПадулы.
18. Политика low-watermark в модели Белла-ЛаПадулы. Примеры реализации запрещенных информационных потоков.
19. Безопасность переходов в БЛ-модели.
20. Модель мандатной политики целостности информации Биба.
21. Модель систем военных сообщений.
22. Автоматная модель безопасности информационных потоков.
23. Программная модель контроля информационных потоков.
24. Вероятностная модель безопасности информационных потоков.
25. Базовая модель ролевого управления доступом.
26. Модель администрирования ролевого управления доступом.
27. Модель мандатного ролевого управления доступом.

Критерии выставления оценки на экзамене

Оценка	**Требования к сформированным компетенциям**
«отлично»	Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении заданий, использует в ответе материал монографической литературы, правильно обосновывает принятое решение, владеет разносторонними навыками и приемами выполнения практических задач по методологии научных исследований.
«хорошо»	Оценка «хорошо» выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения.
«удовлетворительно»	Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его

	деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических работ
«неудовлетворительно»	Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы. Как правило, оценка «неудовлетворительно» ставится студентам, которые не могут продолжить обучение без дополнительных занятий по соответствующей дисциплине.

Оценочные средства для текущей аттестации

№ п/п	Код ОС	Наименование оценочного средства	Кроткая характеристика оценочного средства	Представление оценочного средства в фонде
1	ОУ-1	Собеседование	Средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определённому разделу, теме, проблеме и т.п.	Вопросы по темам/разделам дисциплины
2	ОУ-2	Коллоквиум	Средство контроля усвоения учебного материала темы, раздела или разделов дисциплины, организованное как учебное занятие в виде собеседования преподавателя с обучающимися.	Вопросы по темам/разделам дисциплины
3	ПР-7	Конспект	Продукт самостоятельной работы обучающегося, отражающий основные идеи заслушанной лекции, сообщения и т.д.	Темы/разделы дисциплины