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 4 семестр 8
лекции 36 час.
практические занятия 18 час.
лабораторные работы 18 час.
в том числе с использованием МАО лек. 9 / пр. 0 / лаб. 0 час.
всего часов аудиторной нагрузки 72 час.
в том числе с использованием МАО 9 час.
самостоятельная работа 72 час.
в том числе на подготовку к экзамену 36 час.
контрольные работы (количество) не предусмотрены
курсовая работа / курсовой проект не предусмотрены
зачет не предусмотрен
экзамен 8 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: Власов А.А.

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 , _4_credits
Instructor: *Dobrzhinsky Y.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 regulatory legal acts in their professional activities (OPK-5);

• 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 mathemtical 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. Девянин, П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками [Электронный ресурс] :

учебно-методическое пособие / П.Н. Девянин. — Электрон. дан. — Москва : Горячая линия-Телеком, 2012. — 320 с. — режим доступа: https://e.lanbook.com/book/5150#authors

2. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях: Учебное пособие / Иванов М.А., Чугунков И.В. - М.:НИЯУ "МИФИ", 2012. - 400 с. — Режим доступа: http://znanium.com/catalog/product/562922

3. Каляева И.А., Информационно-телекоммуникационные и компьютерные технологии, устройства и системы: состояние и перспективы развития в Южном федеральном университете [Электронный ресурс] / Каляева И.А., Кухаренко А.П. - Ростов н/Д : Изд-во ЮФУ, 2010. - 520 с. - Режим доступа: h4. ttp://www.studentlibrary.ru/book/ISBN9785927506644.html

4. 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

5. . 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

Form of final control: *exam*

Аннотация к рабочей программе дисциплины

«Модели безопасности компьютерных систем»

Рабочая программа учебной дисциплины «Модели безопасности компьютерных систем»» предназначен для обучения студентов специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит в состав дисциплин базовой части учебного плана Б1.Б.12.04.

Общая трудоемкость освоения дисциплины составляет 144 часов (4 з.е.). Учебным планом предусмотрены лекционные занятия (36 час.), лабораторные работы (18 часов), практические занятия (18 часов), самостоятельная работа студента (72 час.). Дисциплина реализуется на 2 курсе в 4 семестре. Форма контроля по дисциплине – экзамен.

Дисциплина логически и содержательно связана с такими курсами, как «Информатика», «Математическая логика и теория алгоритмов», «Дискретная математика», «Основы информационной безопасности»

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);

- способностью использовать нормативные правовые акты в своей профессиональной деятельности (ОПК-5);
- 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 профессиональные и профессионально-специализированные компетенции.

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

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), лабораторные работы (ПР-6).

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	ОПК-7 ОПК-9 ПК-4	знает	собеседование (ОУ-1), коллоквиум (ОУ-2).	1-9

	безопасности компьютерных систем		умеет	лабораторные работы (ПР-6)	1-9
			владеет	конспект (ПР-7),	1-9
2	Раздел II. Модели компьютерных систем с дискреционным управлением доступом	ОПК-7 ОПК-9 ПК-4	знает	собеседование (ОУ-1), коллоквиум (ОУ-2).	10-13
			умеет	лабораторные работы (ПР-6)	10-13
			владеет	конспект (ПР-7),	10-13
3	Раздел III. Модели изолированной программной среды	ОПК-7 ОПК-9 ПК-4	знает	собеседование (ОУ-1), коллоквиум (ОУ-2).	14-16
			умеет	лабораторные работы (ПР-6)	14-16
			владеет	конспект (ПР-7),	14-16
4	Раздел IV. Модели компьютерных систем с мандатным управлением доступом	ОПК-7 ОПК-9 ПК-4	знает	собеседование (ОУ-1), коллоквиум (ОУ-2).	17-21
			умеет	лабораторные работы (ПР-6)	17-21
			владеет	конспект (ПР-7),	17-21
5	Раздел V. Модели безопасности информационных потоков	ОПК-7 ОПК-9 ПК-4	знает	собеседование (ОУ-1), коллоквиум (ОУ-2).	22-24
			умеет	лабораторные работы	22-24

				(ПР-6)	
			владеет	конспект (ПР-7),	22-24
6	Раздел VI. Модели компьютерных систем с ролевым управлением доступом	ОПК-7 ОПК-9 ПК-4	знает	собеседование (ОУ-1), коллоквиум (ОУ-2).	25-27
			умеет	лабораторные работы (ПР-6)	25-27
			владеет	конспект (ПР-7),	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. Девянин, П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками [Электронный ресурс] : учебно-методическое пособие / П.Н. Девянин. — Электрон. дан. — Москва : Горячая линия-Телеком, 2012. — 320 с. — режим доступа: https://e.lanbook.com/book/5150#authors

2. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях: Учебное пособие / Иванов М.А., Чугунков И.В. - М.:НИЯУ "МИФИ", 2012. - 400 с. — Режим доступа: http://znanium.com/catalog/product/562922

3. Каляева И.А., Информационно-телекоммуникационные и компьютерные технологии, устройства и системы: состояние и перспективы развития в Южном федеральном университете [Электронный ресурс] / Каляева И.А., Кухаренко А.П. - Ростов н/Д : Изд-во ЮФУ, 2010. - 520 с. - Режим доступа: h4. ttp://www.studentlibrary.ru/book/ISBN9785927506644.html

4. 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

5. . 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

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. Вичугова А.А. Инструментальные средства разработки компьютерных систем и комплексов [Электронный ресурс]: учебное пособие для СПО/ Вичугова А.А.— Электрон. текстовые данные.— Саратов: Профобразование, 2017.— 135 с.— Режим доступа: http://www.iprbookshop.ru/66387.html

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

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.

VI. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Количество аудиторных часов, отведенных на изучение дисциплины «Модели безопасности компьютерных систем», составляет 72 часа. На самостоятельную работу – 72 часа. При этом аудиторная нагрузка состоит из 36 лекционных часов, 18 часов практических занятий и 18 часов лабораторных работ.

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 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 «Модели безопасности компьютерных систем»
Специальность 10.05.01 Компьютерная безопасность
(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 недели обучения	Подготовка практических заданий 1- 6	36	Отчет о выполнении
2	Сессия	Подготовка к экзамену	36	Экзамен

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»
Специальность 10.05.01 Компьютерная безопасность
(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

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	собеседование (ОУ-1), коллоквиум (ОУ-2).	1-9
			умеет	лабораторные работы (ПР-6)	1-9
			владеет	конспект (ПР-7),	1-9
2	Раздел II. Модели компьютерных систем с дискреционным управлением доступом	ОПК-7 ОПК-9 ПК-4	знает	собеседование (ОУ-1), коллоквиум (ОУ-2).	10-13
			умеет	лабораторные работы (ПР-6)	10-13
			владеет	конспект (ПР-7),	10-13
3	Раздел III. Модели изолированной программной среды	ОПК-7 ОПК-9 ПК-4	знает	собеседование (ОУ-1), коллоквиум (ОУ-2).	14-16
			умеет	лабораторные	14-16

				работы (ПР-6)	
			владеет	конспект (ПР-7),	14-16
4	Раздел IV. Модели компьютерных систем с мандатным управлением доступом	ОПК-7 ОПК-9 ПК-4	знает	собеседование (ОУ-1), коллоквиум (ОУ-2).	17-21
			умеет	лабораторные работы (ПР-6)	17-21
			владеет	конспект (ПР-7),	17-21
5	Раздел V. Модели безопасности информационных потоков	ОПК-7 ОПК-9 ПК-4	знает	собеседование (ОУ-1), коллоквиум (ОУ-2).	22-24
			умеет	лабораторные работы (ПР-6)	22-24
			владеет	конспект (ПР-7),	22-24
6	Раздел VI. Модели компьютерных систем с ролевым управлением доступом	ОПК-7 ОПК-9 ПК-4	знает	собеседование (ОУ-1), коллоквиум (ОУ-2).	25-27
			умеет	лабораторные работы (ПР-6)	25-27
			владеет	конспект (ПР-7),	22-27
№ 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	ОПК-7 ОПК-9 ПК-4	знает	собеседование (ОУ-1), коллоквиум (ОУ-2).	1-9
			умеет	лаборатор	1-9

	компьютерных систем			ные работы (ПР-6)	
			владеет	конспект (ПР-7),	1-9
2	Раздел II. Модели компьютерных систем с дискреционным управлением доступом	ОПК-7 ОПК-9 ПК-4	знает	собеседование (ОУ-1), коллоквиум (ОУ-2).	10-13
			умеет	лабораторные работы (ПР-6)	10-13
			владеет	конспект (ПР-7),	10-13
3	Раздел III. Модели изолированной программной среды	ОПК-7 ОПК-9 ПК-4	знает	собеседование (ОУ-1), коллоквиум (ОУ-2).	14-16
			умеет	лабораторные работы (ПР-6)	14-16
			владеет	конспект (ПР-7),	14-16
4	Раздел IV. Модели компьютерных систем с мандатным управлением доступом	ОПК-7 ОПК-9 ПК-4	знает	собеседование (ОУ-1), коллоквиум (ОУ-2).	17-21
			умеет	лабораторные работы (ПР-6)	17-21
			владеет	конспект (ПР-7),	17-21
5	Раздел V. Модели безопасности информационных потоков	ОПК-7 ОПК-9 ПК-4	знает	собеседование (ОУ-1), коллоквиум (ОУ-2).	22-24
			умеет	лабораторные работы (ПР-6)	22-24

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

Шкала оценивания уровня сформированности компетенций

Код и формулировка компетенции	**Этапы формирования компетенции**		**критерии**	**показатели**
(ОПК-7) способностью учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специально	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.	полнота и системность знаний	изложение полученных знаний полное, в соответствии с требованиями учебной программы; ошибки отсутствуют или несущественны, обучающийся способен самостоятельно исправить.
	Умеет	Осуществлять подбор, изучение и обобщение научно-технической информации,	степень самостоятельности выполнения	обучающийся способен свободно строить модели

го назначения		нормативных и методических материалов по методам обеспечения информационной безопасности компьютерных систем.	действия (умения); осознанность действия (умения).	простых неформализуемых задач самостоятельно; свободно отвечает на вопросы, касающиеся выполняемых действий.
	Владеет	Навыком формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем	степень умения отбирать и интегрировать имеющиеся знания и навыки исходя из поставленной цели, проводить самоанализ и самооценку.	обучающийся способен самостоятельно создать вычислительную сеть для решения прикладных инженерных задач.
(ОПК-9) способностью разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности	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.	полнота и системность знаний	изложение полученных знаний полное, в соответствии с требованиями учебной программы; ошибки отсутствуют или несущественны, обучающийся способен самостоятельно исправить.

информации	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.	степень самостоятельности выполнения действия (умения); осознанность действия (умения).	обучающийся способен свободно строить модели простых неформализуемых задач самостоятельно; свободно отвечает на вопросы, касающиеся выполняемых действий.
	Владеет	Методами разработки частных политик безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками.	степень умения отбирать и интегрировать имеющиеся знания и навыки исходя из поставленной цели, проводить самоанализ и самооценку.	обучающийся способен самостоятельно создать вычислительную сеть для решения прикладных инженерных задач.

№ 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	Практические задания (ПР-9)	1-9
			Умеет	Практические задания (ПР-9)	1-9
			владеет	Практические задания (ПР-9)	1-9
2	Раздел II. Модели компьютерных систем с дискреционным управлением доступом	ОПК-7 ОПК-9 ПК-4	знает	Практические задания (ПР-9)	10-13
			Умеет	Практические задания (ПР-9)	10-13
			владеет	Практические задания (ПР-9)	10-13
3	Раздел III. Модели изолированной программной среды	ОПК-7 ОПК-9 ПК-4	знает	Практические задания	14-16

				(ПР-9)	
			Умеет	Практические задания (ПР-9)	14-16
			владеет	Практические задания (ПР-9)	14-16
4	Раздел IV. Модели компьютерных систем с мандатным управлением доступом	ОПК-7 ОПК-9 ПК-4	знает	Практические задания (ПР-9)	17-21
			Умеет	Практические задания (ПР-9)	17-21
			владеет	Практические задания (ПР-9)	17-21
5	Раздел V. Модели безопасности информационных потоков	ОПК-7 ОПК-9 ПК-4	знает	Практические задания (ПР-9)	22-24
			Умеет	Практические задания (ПР-9)	22-24
			владеет	Практические задания (ПР-9)	22-24
6	Раздел VI. Модели компьютерных систем с ролевым управлением доступом	ОПК-7 ОПК-9 ПК-4	знает	Практические задания (ПР-9)	25-27
			Умеет	Практические задания (ПР-9)	25-27
			владеет	Практические задания (ПР-9)	22-27

Методические рекомендации, определяющие процедуры оценивания результатов освоения дисциплины

Промежуточная форма аттестации по данной дисциплине - экзамен. Для допуска к экзамену необходимо сдать все практические задания. В случае, если ко дню проведения экзамена обучающийся не сдал какие-либо из практических заданий, он получает возможность сдать их на консультации перед экзаменом. Экзамен выставляется на основании сдачи всех практических заданий и сдачи экзаменационного билета.

При определении оценки ответа обучающегося как на экзамене, так и на практическом занятии учитываются:

- соблюдение норм литературной речи;
- полнота и содержательность ответа;
- умение привести примеры;
- умение пользоваться дополнительной литературой при подготовке к занятиям;
- соответствие представленной в ответах информации материалам лекций и учебной литературы, актуальным сведениям из информационных ресурсов Интернет.

Оценочные средства для промежуточной аттестации

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.

Оценочные средства для текущей аттестации

В качестве оценочных средств для текущей аттестации применяются конспект (ПР-7).

Конспект является показателем сформированности компетенции на пороговом уровне. Темы конспектов соответствуют темам теоретической части курса из Раздела II РПУД. Критерии оценки по данному виду оценочных средств представлены в таблице:

Оценка	Содержание конспекта
Отлично	Конспект содержит все понятия, термины, положения, изученные на лекции и/или с использованием основных источников литературы, а также содержит сведения из дополнительных источников.
Хорошо	Конспект содержит все понятия, термины, положения, изученные на лекции и/или с использованием основных источников литературы.
Удовлетворительно	Конспект содержит базовые понятия, термины,

	положения, изученные на лекции.
Неудовлетворительно	Конспект не содержит основных понятий, терминов, положений по данной теме.