МИНОБРНАУКИ РОССИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рабочая программа дисциплины (модуля)

МОДЕЛИ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ

Специальность и специализация
10.05.03 Информационная безопасность автоматизированных систем. Безопасность открытых информационных систем

Год набора на ОПОП
2025

Форма обучения
очная

Владивосток 2025

Рабочая программа дисциплины (модуля) «Модели безопасности компьютерных систем» составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 10.05.03 Информационная безопасность автоматизированных систем (утв. приказом Минобрнауки России от 26.11.2020г. №1457) и Порядком организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры (утв. приказом Минобрнауки России от 06.04.2021 г. N245).

Составитель(и):

Шумик Е.Г., кандидат экономических наук, заведующий кафедрой, Кафедра информационной безопасности, Ekaterina.Shumik1@vvsu.ru

Утверждена на заседании кафедры информационной безопасности от 15.05.2025 , протокол № 9

СОГЛАСОВАНО:

Заведующий кафедрой (разработчика)

Шумик Е.Г.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ	
Сертификат	eg_1575874368
Номер транзакции	0000000000EA7C58
Владелец	Шумик Е.Г.

1 Цель, планируемые результаты обучения по дисциплине (модулю)

Целью изучения дисциплины «Модели безопасности компьютерных систем»является теоретическая и практическая подготовка специалистов к деятельности, связаннойс защитой информации; обучение общим принципам построения моделей безопасности иполитик безопасности, основным методам исследования корректности систем защиты,методологии обследования и проектирования систем защиты.

Задачами дисциплины являются:

- изложение теоретических основ компьютерной безопасности;
- описание моделей безопасности информационных систем;
- описание моделей доступа в информационных системах;
- обучение методологии обследования и проектирования систем защиты;
- обучение навыкам настройки основных компонентов систем защиты и примененияхтехнологий защиты.

Планируемыми результатами обучения по дисциплине (модулю), являются знания, умения, навыки. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы, представлен в таблице 1.

Таблица 1 – Компетенции, формируемые в результате изучения дисциплины (модуля)

Название ОПОП ВО, сокращенное	Код и формулировка компетенции	Код и формулировка индикатора достижения компетенции	Результаты обучения по дисциплине		
			Код результата	Формулировка результата	
10.05.03 «Информационная безопасность автоматизированных систем» (ИБ)	ОПК-5.1 : Способен разрабатывать и реализовывать политику информационной безопасности открытых информационных систем;	ОПК-5.1.1к : определяет источники информации, регламентирующие деятельность, связанную с организацией политики безопасности	РД1	Знание	основные угрозы безопасности информации и модели нарушителя в информационных системах; принципы формирования политики информационной безопасности в информационных системах
			РД2	Умение	реализовывать основные модели доступа в информационной системе
			РД3	Навык	разработки элементов политики информационной безопасности автоматизированной системы

В процессе освоения дисциплины решаются задачи воспитания гармонично развитой, патриотичной и социально ответственной личности на основе традиционных российских духовно-нравственных и культурно-исторических ценностей, представленные в таблице 1.2.

Таблица 1.2 – Целевые ориентиры воспитания

Воспитательные задачи	Формирование ценностей	Целевые ориентиры
Формирование гражданской позиции и патриотизма		
Воспитание уважения к истории и культуре России	Гражданственность	Гибкость мышления
Формирование духовно-нравственных ценностей		
Воспитание чувства долга и ответственности перед семьей и обществом	Справедливость	Дисциплинированность
Формирование научного мировоззрения и культуры мышления		
Развитие познавательного интереса и стремления к знаниям	Гражданственность	Осознание ценности профессии
Формирование коммуникативных навыков и культуры общения		
Воспитание культуры диалога и уважения к мнению других людей	Гражданственность	Индивидуальность

2 Место дисциплины (модуля) в структуре ОПОП

Дисциплина «Модели безопасности компьютерных систем» относится квариативной части дисциплин учебного плана направления «Информационнаябезопасность автоматизированных систем».Входными требованиями, необходимыми для освоения дисциплины, являетсяналичие у обучающихся компетенций, сформированных при изучении дисциплин и/илипрохождении практик «Безопасность операционных систем», «Безопасность систем базданных», «Информатика и основы программирования», «Основы информационнойбезопасности». На данную дисциплину опираются «Защита выпускной квалификационнойработы, включая подготовку к процедуре защиты и процедуру защиты», «Защита программи данных», «Программно-аппаратные средства защиты информации».

3. Объем дисциплины (модуля)

Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу с обучающимися (по видам учебных занятий) и на самостоятельную работу, приведен в таблице 2.

Таблица 2 – Общая трудоемкость дисциплины

Название ОПОП ВО	Форма обуче-ния	Часть УП	Семестр (ОФО) или курс (ЗФО, ОЗФО)	Трудо-емкость	Объем контактной работы (час)						СРС	Форма аттес-тации
				(З.Е.)	Всего	Аудиторная			Внеауди-торная			
						лек.	прак.	лаб.	ПА	КСР		
10.05.03 Информационная безопасность	ОФО	С1.Б	7	5	75	36	18	0	1	20	105	Э

автоматизированных систем												

4 Структура и содержание дисциплины (модуля)

4.1 Структура дисциплины (модуля) для ОФО

Тематический план, отражающий содержание дисциплины (перечень разделов и тем), структурированное по видам учебных занятий с указанием их объемов в соответствии с учебным планом, приведен в таблице 3.1

Таблица 3.1 – Разделы дисциплины (модуля), виды учебной деятельности и формы текущего контроля для ОФО

№	Название темы	Код результата обучения	Кол-во часов, отведенное на				Форма текущего контроля
			Лек	Практ	Лаб	СРС	
1	Введение в дисциплину.	РД1, РД2, РД3	6	2	0	20	практическое задание
2	Модели компьютерных систем с дискреционным управлением	РД1, РД2, РД3	10	4	0	17	практическое задание
3	Модели компьютерных систем с мандатным управлением доступом	РД1, РД2, РД3	8	4	0	17	практическое задание
4	Модели безопасности информационных потоков и изолированной программной среды.	РД1, РД2, РД3	4	2	0	17	практическое задание
5	Модели компьютерных систем с ролевым управлением доступом	РД1, РД2, РД3	4	2	0	17	практическое задание
6	Развитие формальных моделей безопасности компьютерных систем	РД1, РД2, РД3	4	4	0	17	практическое задание
Итого по таблице			**36**	**18**	**0**	**105**	

4.2 Содержание разделов и тем дисциплины (модуля) для ОФО

Тема 1 Введение в дисциплину.

Содержание темы: Основные элементы теории компьютерной безопасности (сущность, субъект, доступ, право доступа, информационные потоки по памяти или по времени). Основная аксиома. Проблема построения защищенной КС. Модели ценности информации: аддитивная модель, порядковая шкала, решетка многоуровневой безопасности. Угрозы безопасности информации. Политика безопасности Классификация угроз безопасности информации. Угрозы конфиденциальности, целостности, доступности информации, раскрытия параметров КС. Понятие политики безопасности. Модель нарушителя. Основные виды политик управления доступом и информационными потоками. Политики дискреционного, мандатного, ролевого управления доступом, изолированной программной среды и безопасности информационных потоков.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: лекция, практическое занятие.

Виды самостоятельной подготовки студентов по теме: подготовка к практическому занятию.

Тема 2 Модели компьютерных систем с дискреционным управлением.

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

Харрисона-Руззо-Ульмана (ХРУ). Анализ безопасности систем ХРУ. Монооперационные системы ХРУ. Алгоритмическая неразрешимость задачи проверки безопасности систем ХРУ Модель типизированной матрицы доступов (ТМД). Монотонные системы ТМД и их каноническая форма. Граф создания. Ациклические монотонные ТМД и алгоритм проверки их безопасности. Модель типизированной матрицы доступов (ТМД). Монотонные системы ТМД и их каноническая форма. Граф создания. Ациклические монотонные ТМД и алгоритм проверки их безопасности. Классическая модель Take-Grant. Де-юре правила преобразования графов доступов. Условия передачи прав доступа в графе доступов, состоящем только из субъектов. Остров, мост, пролеты моста. Условия передачи прав доступа в произвольном графе доступов при отсутствии ограничений на кооперацию субъектов. Классическая модель Take-Grant. Де-юре правила преобразования графов доступов. Условия передачи прав доступа в графе доступов, состоящем только из субъектов. Остров, мост, пролеты моста. Условия передачи прав доступа в произвольном графе доступов при отсутствии ограничений на кооперацию субъектов. Расширенная модель Take-Grant. Де-факто правила преобразования графов доступов и информационных потоков. Условия реализации информационных потоков. Алгоритм построения замыкания графа доступов и информационных потоков. Представление систем Take-Grant системами ХРУ и ТМД. Расширенная модель Take-Grant. Де-факто правила преобразования графов доступов и информационных потоков. Условия реализации информационных потоков. Алгоритм построения замыкания графа доступов и информационных потоков. Представление систем Take-Grant системами ХРУ и ТМД.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: лекция, практическое занятие.

Виды самостоятельной подготовки студентов по теме: подготовка к практическому занятию.

Тема 3 Модели компьютерных систем с мандатным управлением доступом.

Содержание темы: Классическая модель Белла-ЛаПадулы. Свойства безопасности. Безопасный доступ, состояние, система. Базовая теорема безопасности. Интерпретации модели Белла-ЛаПадулы: модель реализации политики low-watermark, безопасность переходов, модель мандатной политики целостности информации Биба. Недостатки модели Белла-ЛаПадулы. Классическая модель Белла-ЛаПадулы. Свойства безопасности. Безопасный доступ, состояние, система. Базовая теорема безопасности. Интерпретации модели Белла-ЛаПадулы: модель реализации политики low-watermark, безопасность переходов, модель мандатной политики целостности информации Биба. Недостатки модели Белла-ЛаПадулы. Примеры реализации запрещенных информационных потоков. Интерпретации модели Белла-ЛаПадулы: модель реализации политики low-watermark, безопасность переходов, модель мандатной политики целостности информации Биба. Недостатки модели Белла-ЛаПадулы. Примеры реализации запрещенных информационных потоков по памяти или по времени. Интерпретации модели Белла-ЛаПадулы: модель реализации политики low-watermark, безопасность переходов, модель мандатной политики целостности информации Биба. Недостатки модели Белла-ЛаПадулы. Неформальное и формальное описания модели систем военных сообщений.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: лекция, практическое занятие.

Виды самостоятельной подготовки студентов по теме: подготовка к практическому занятию.

Тема 4 Модели безопасности информационных потоков и изолированной программной среды.

Содержание темы: Автоматная модель безопасности информационных потоков. Программная модель контроля информационных потоков. Контролирующий механизм

защиты. Вероятностная модель безопасности информационных потоков. «Информационное невлияние». Автоматная модель безопасности информационных потоков. Программная модель контроля информационных потоков. Контролирующий механизм защиты. Вероятностная модель безопасности информационных потоков. «Информационное невлияние». Субъектно-ориентированная модель изолированной программной среды (ИПС). Объекты, функционально ассоциированные с субъектами. Мониторы безопасности обращений и порождения субъектов. Базовая теорема ИПС. Субъектно-ориентированная модель изолированной программной среды (ИПС). Объекты, функционально ассоциированные с субъектами. Мониторы безопасности обращений и порождения субъектов. Базовая теорема ИПС .

Формы и методы проведения занятий по теме, применяемые образовательные технологии: лекция, практическое занятие.

Виды самостоятельной подготовки студентов по теме: подготовка к практическому занятию.

Тема 5 Модели компьютерных систем с ролевым управлением доступом.

Содержание темы: Описание базовой модели ролевого управления доступом. Иерархия ролей. Механизм ограничений. Модель администрирования ролевого управления доступом. Администрирование множеств авторизованных ролей пользователей, прав доступа, которыми обладает роли, иерархии ролей. Модель мандатного ролевого управления доступом. Задание иерархии ролей и ограничений в соответствии с требованиями либерального или строгого мандатного управления доступом. Безопасность информационных потоков. Защита от угроз конфиденциальности и целостности информации.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: лекция, практическое занятие.

Виды самостоятельной подготовки студентов по теме: подготовка к практическому занятию.

Тема 6 Развитие формальных моделей безопасности компьютерных систем.

Содержание темы: Взаимосвязь положений классических формальных моделей безопасности КС. Критический анализ классических моделей. Проблема адекватности реализации модели безопасности в реальной КС. Развитие формальных моделей. Обзор семейства формальных моделей управления доступом и информационными потоками (ДП-моделей) КС с дискреционным, мандатным или ролевым управлением доступом. Доверенные и недоверенные субъекты. Анализ информационных потоков по памяти или по времени. Функционально или параметрически ассоциированные с субъектами сущности. Обзор семейства формальных моделей управления доступом и информационными потоками (ДП-моделей) КС с дискреционным, мандатным или ролевым управлением доступом. Доверенные и недоверенные субъекты. Анализ информационных потоков по памяти или по времени. Функционально или параметрически ассоциированные с субъектами сущности.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: лекция, практическое занятие.

Виды самостоятельной подготовки студентов по теме: подготовка к практическому занятию.

5 Методические указания для обучающихся по изучению и реализации дисциплины (модуля)

5.1 Методические рекомендации обучающимся по изучению дисциплины и по обеспечению самостоятельной работы

Самостоятельная работа студентов (СРС) — это деятельность учащихся, которую они совершают без непосредственной помощи и указаний преподавателя, руководствуясь сформировавшимися ранее представлениями о порядке и правильности выполнения операций. Цель СРС в процессе обучения заключается, как в усвоении знаний, так и в формировании умений и навыков по их использованию в новых условиях на новом учебном материале. Самостоятельная работа призвана обеспечивать возможность осуществления студентами самостоятельной познавательной деятельности в обучении, и является видом учебного труда, способствующего формированию у студентов самостоятельности. В данной учебной программе приведен перечень основных и дополнительных источников, которые предлагается изучить в процессе облучения по дисциплине. Кроме того, для расширения и углубления знаний по данной дисциплине целесообразно использовать: научные публикации в тематических журналах; полнотекстовые базы данных библиотеки; имеющиеся в библиотеках вуза и региона публикаций на электронных и бумажных носителях. Успешное освоение дисциплины предполагает активную работу студентов на всех занятиях аудиторной формы: лекций и практических занятий, выполнение аттестационный мероприятий, эффективную самостоятельную работу. В процессе изучения дисциплины студенту необходимо ориентироваться на самостоятельную проработку лекционного материала, подготовку к практическим занятиям, выполнение тестов, самостоятельное изучение некоторых разделов курса Для проведения занятий лекционного типа используются учебно-наглядные пособия в форме презентационных материалов, обеспечивающих тематические иллюстрации, соответствующие темам лекций, представленным в пункте 4 настоящей РПД

5.2 Особенности организации обучения для лиц с ограниченными возможностями здоровья и инвалидов

При необходимости обучающимся из числа лиц с ограниченными возможностями здоровья и инвалидов (по заявлению обучающегося) предоставляется учебная информация в доступных формах с учетом их индивидуальных психофизических особенностей:

- для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания, консультации и др.
- для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания, консультации и др.
- для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; индивидуальные задания, консультации и др.

6 Фонд оценочных средств для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине (модулю)

В соответствии с требованиями ФГОС ВО для аттестации обучающихся на соответствие их персональных достижений планируемым результатам обучения по дисциплине (модулю) созданы фонды оценочных средств. Типовые контрольные задания,

методические материалы, определяющие процедуры оценивания знаний, умений и навыков, а также критерии и показатели, необходимые для оценки знаний, умений, навыков и характеризующие этапы формирования компетенций в процессе освоения образовательной программы, представлены в Приложении 1.

7 Учебно-методическое и информационное обеспечение дисциплины (модуля)

7.1 Основная литература

1. Кировский, О. М. Вероятностные модели при анализе безопасности критических систем : учебно-методическое пособие / О. М. Кировский, А. С. Королев, О. С. Сунцов. — Москва : РТУ МИРЭА, 2025. — 58 с. — ISBN 978-5-7339-2486-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/493511 (дата обращения: 27.10.2025). — Режим доступа: для авториз. пользователей.
2. Фомина, К. Ю. Модели угроз и нарушителей безопасности информации объектов информатизации : учебное пособие / К. Ю. Фомина, Ю. В. Конкин, В. А. Севостьянов. — Рязань : РГРТУ, 2024 — Часть 1— 2024. — 88 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/494567 (дата обращения: 27.10.2025). — Режим доступа: для авториз. пользователей.

7.2 Дополнительная литература

1. Гисин, В. Б. Криптография и распределенные реестры : учебное пособие : [16+] / В. Б. Гисин ; Финансовый университет при Правительстве Российской Федерации. – Москва : Прометей, 2022. – 186 с. : табл., схем. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=700941 (дата обращения: 20.10.2025). – Библиогр. в кн. – ISBN 978-5-00172-257-1. – Текст : электронный.
2. Попов, И. В. Информационная безопасность : практикум / И. В. Попов, Н. И. Улендеева. - Самара : Самарский юридический институт ФСИН России, 2022. - 90 с. - ISBN 978-5-91612-375-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/2016193 (Дата обращения - 22.10.2025)

7.3 Ресурсы информационно-телекоммуникационной сети "Интернет", включая профессиональные базы данных и информационно-справочные системы (при необходимости):

1. Электронно-библиотечная система "ZNANIUM.COM"
2. Электронно-библиотечная система "ЛАНЬ"
3. Электронно-библиотечная система "УНИВЕРСИТЕТСКАЯ БИБЛИОТЕКА ОНЛАЙН"
4. Open Academic Journals Index (OAJI). Профессиональная база данных - Режим доступа: http://oaji.net/
5. Президентская библиотека им. Б.Н.Ельцина (база данных различных профессиональных областей) - Режим доступа: https://www.prlib.ru/
6. Информационно-справочная система "Консультант Плюс" - Режим доступа: http://www.consultant.ru/

8 Материально-техническое обеспечение дисциплины (модуля) и перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения

Основное оборудование:

- Компьютеры
- Проектор

Программное обеспечение:

- Microsoft Office Professional Plus 2010

МИНОБРНАУКИ РОССИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Фонд оценочных средств
для проведения текущего контроля
и промежуточной аттестации по дисциплине (модулю)

МОДЕЛИ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ

Специальность и специализация
10.05.03 Информационная безопасность автоматизированных систем. Безопасность открытых информационных систем

Год набора на ОПОП
2025

Форма обучения
очная

Владивосток 2025

1 Перечень формируемых компетенций

Название ОПОП ВО, сокращенное	Код и формулировка компетенции	Код и формулировка индикатора достижения компетенции
10.05.03 «Информационная безопасность автоматизированных систем» (ИБ)	ОПК-5.1 : Способен разрабатывать и реализовывать политику информационной безопасности открытых информационных систем;	ОПК-5.1.1к : определяет источники информации, регламентирующие деятельность, связанную с организацией политики безопасности

Компетенция считается сформированной на данном этапе в случае, если полученные результаты обучения по дисциплине оценены положительно (диапазон критериев оценивания результатов обучения «зачтено», «удовлетворительно», «хорошо», «отлично»). В случае отсутствия положительной оценки компетенция на данном этапе считается несформированной.

2 Показатели оценивания планируемых результатов обучения

Компетенция ОПК-5.1 «Способен разрабатывать и реализовывать политику информационной безопасности открытых информационных систем;»

Таблица 2.1 – Критерии оценки индикаторов достижения компетенции

Код и формулировка индикатора достижения компетенции	Результаты обучения по дисциплине			Критерии оценивания результатов обучения
	Код рез-та	Тип рез-та	Результат	
ОПК-5.1.1к : определяет источники информации, регламентирующие деятельность, связанную с организацией политики безопасности	РД 1	Знание	основные угрозы безопасности информации и модели нарушителя в информационных системах; принципы формирования политики информационной безопасности в информационных системах	решение тестовых заданий
	РД 2	Умение	реализовывать основные модели доступа в информационной системе	решение тестовых заданий
	РД 3	Навык	разработки элементов политики информационной безопасности автоматизированной системы	решение тестовых заданий

Таблица заполняется в соответствии с разделом 1 Рабочей программы дисциплины (модуля).

3 Перечень оценочных средств

Таблица 3 – Перечень оценочных средств по дисциплине (модулю)

Контролируемые планируемые результаты обучения		Контролируемые темы дисциплины	Наименование оценочного средства и представление его в ФОС	
			Текущий контроль	Промежуточная аттестация
Очная форма обучения				
РД1	Знание : основные угрозы безопасности информации и модели нарушителя в информационных системах; принципы формирования политики информационной безопасности в информационных системах	1.1. Введение в дисциплину.	Тест	Экзамен в устной форме
		1.2. Модели компьютерных систем с дискреционным управлением	Тест	Экзамен в устной форме
		1.3. Модели компьютерных систем с мандатным управлением доступом	Тест	Экзамен в устной форме
		1.4. Модели безопасности информационных потоков и изолированной программной среды.	Тест	Экзамен в устной форме
		1.5. Модели компьютерных систем с ролевым управлением доступом	Тест	Экзамен в устной форме
		1.6. Развитие формальных моделей безопасности компьютерных систем	Тест	Экзамен в устной форме
РД2	Умение : реализовывать основные модели доступа в информационной системе	1.1. Введение в дисциплину.	Практическая работа	Экзамен в устной форме
		1.2. Модели компьютерных систем с дискреционным управлением	Практическая работа	Экзамен в устной форме
		1.3. Модели компьютерных систем с мандатным управлением доступом	Практическая работа	Экзамен в устной форме
		1.4. Модели безопасности информационных потоков и изолированной программной среды.	Практическая работа	Экзамен в устной форме
		1.5. Модели компьютерных систем с ролевым управлением доступом	Практическая работа	Экзамен в устной форме
		1.6. Развитие формальных моделей безопасности компьютерных систем	Практическая работа	Экзамен в устной форме
РД3	Навык : разработки элементов политики информационной безопасности автоматизированной системы	1.1. Введение в дисциплину.	Практическая работа	Экзамен в устной форме
		1.2. Модели компьютерных систем с дискреционным управлением	Практическая работа	Экзамен в устной форме
		1.3. Модели компьютерных систем с мандатным управлением доступом	Практическая работа	Экзамен в устной форме
		1.4. Модели безопасности информационных потоков и изолированной программной среды.	Практическая работа	Экзамен в устной форме

		1.5. Модели компьютерных систем с ролевым управлением доступом	Практическая работа	Экзамен в устной форме
		1.6. Развитие формальных моделей безопасности компьютерных систем	Практическая работа	Экзамен в устной форме

4 Описание процедуры оценивания

Качество сформированности компетенций на данном этапе оценивается по результатам текущих и промежуточных аттестаций при помощи количественной оценки, выраженной в баллах. Максимальная сумма баллов по дисциплине (модулю) равна 100 баллам.

Вид учебной деятельности	Оценочное средство			
	Тест 1-5	Практическая работа	Экзамен	Итого
Лекционные занятия	20			80
Практические занятия		60		
Промежуточная аттестация			20	20
Итого	20	60	20	100

Сумма баллов, набранных студентом по всем видам учебной деятельности в рамках дисциплины, переводится в оценку в соответствии с таблицей.

Сумма баллов по дисциплине	Оценка по промежуточной аттестации	Характеристика качества сформированности компетенции
от 91 до 100	«зачтено» / «отлично»	Студент демонстрирует сформированность дисциплинарных компетенций, обнаруживает всестороннее, систематическое и глубокое знание учебного материала, усвоил основную литературу и знаком с дополнительной литературой, рекомендованной программой, умеет свободно выполнять практические задания, предусмотренные программой, свободно оперирует приобретенными знаниями, умениями, применяет их в ситуациях повышенной сложности.
от 76 до 90	«зачтено» / «хорошо»	Студент демонстрирует сформированность дисциплинарных компетенций: основные знания, умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
от 61 до 75	«зачтено» / «удовлетворительно»	Студент демонстрирует сформированность дисциплинарных компетенций: в ходе контрольных мероприятий допускаются значительные ошибки, проявляется отсутствие отдельных знаний, умений, навыков по некоторым дисциплинарным компетенциям, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.
от 41 до 60	«не зачтено» / «неудовлетворительно»	У студента не сформированы дисциплинарные компетенции, проявляется недостаточность знаний, умений, навыков.
от 0 до 40	«не зачтено» / «неудовлетворительно»	Дисциплинарные компетенции не сформированы. Проявляется полное или практически полное отсутствие знаний, умений, навыков.

5 Примерные оценочные средства

5.1 Контрольный тест

1.Какие виды политик информационной безопасности рассматриваются в теории компьютерной безопасности (отметьте один или несколько ответов).

1) мандатная
2) древовидная
3) многоуровневая
4) ролевая

5) дискреционная

6) дискретизированная

7) ничего из перечисленного

2. Как формулируется основная аксиома теории компьютерной безопасности?

1) Все вопросы безопасности информации в КС описываются перечнем субъектов и объектов;

2) Все вопросы безопасности информации в КС описываются уровнями субъектов и объектов;

3) Все вопросы безопасности информации в КС описываются доступами субъектов к объектам;

4) Все вопросы безопасности информации в КС описываются доступами субъектов к субъектам;

5) Все вопросы безопасности информации в КС описываются уровнями доступа субъектов и уровнями безопасности объектов;

6) ничего из перечисленного.

3.Какие из перечисленных моделей являются дискреционными?

1) Модель Биба;

2) Модель Харрисона-Руззо-Ульмана;

3) Модель Белла-ЛаПадулы;

4) Модель Take-Grant;

5) Модель систем военных сообщений;

6) Модель изолированной программной среды.

4. Существует ли алгоритм проверки безопасности систем ХРУ?

1) Да, существует для общего случая;

2) Нет, не существует ни для каких ХРУ;

3) Существует только для монооперационных ХРУ;

4) Существует для некоторых разновидностей ХРУ, а в общем случае – возможно существует, но

не найден;

5) Существует для некоторых разновидностей ХРУ, а в общем случае доказано, что не существует.

6) Вопрос о существовании или не существовании такого алгоритма не решен ни для каких ХРУ.

5. Какие из перечисленных правил являются де-факто правилами расширенной модели Take-Grant?

1) take

2) grant

3) write

4) read

5) spy

6) find

7) post

8) pass

9) invoke

10) observe

Краткие методические указания

Тестовые задания состоят из вопроса и нескольких вариантов ответа. Решение представляет собойуказание номера вопроса и букву, которой обозначен правильный, по мнению студента, вариантответа. В течение семестра проводится 5 тестов по 3 темам на лекционных занятиях, в каждомтесте 16 вопросов.

Шкала оценки

Оценка	Баллы	Описание
5	5	Студент допустил не более 2х ошибок

4	4	Студент совершил от 3 до 6 ошибок в ответах на тест
3	2-3	Студент совершил от 7 до 10 ошибок в ответах на тест
2	0-1	Студент совершил 11 и более ошибок в ответах на тест

5.2 Примеры заданий для выполнения практических работ

Задание №1: Анализ уязвимости сети организации

Цель: Провести аудит информационной инфраструктуры условной организации на предмет выявления потенциальных угроз и уязвимых мест.

Задания:

- Определить структуру корпоративной сети предприятия (топология, используемые протоколы, устройства).
- Выполнить сканирование сетевых ресурсов и сервисов (например, с использованием Nmap).
- Оценить потенциальные угрозы и атаки, исходя из полученных результатов анализа.
- Составить отчет с рекомендациями по повышению уровня защищенности сети.

Задание №2: Проектирование модели защиты информации на предприятии

Цель: Разработать модель защиты информации для конкретного подразделения крупной компании.

Задания:

- Выявить ключевые активы информации подразделения.
- Определить возможные угрозы для каждого актива (угрозы внутренних пользователей, внешние угрозы).
- Предложить меры по защите активов (организационные, административные, технические).
- Создать схему взаимодействия элементов системы защиты.

Задание №3: Реализация двухфакторной аутентификации

Цель: Реализовать систему двухфакторной аутентификации для входа в локальное приложение или веб-сервис.

Задания:

- Настроить сервер приложений с поддержкой аутентификации на основе пароля и дополнительного фактора (смартфон, токены).
- Продемонстрировать работоспособность схемы на практике (регистрация нового пользователя, вход с применением второго фактора).
- Подготовить руководство администратора по настройке и эксплуатации системы.

Задание №4: Исследование механизмов контроля целостности данных

Цель: Изучить механизмы обеспечения целостности данных на примере реализации хеш-функций и цифровых подписей.

Задания:

- Ознакомиться с основными методами криптографического контроля целостности (MD5, SHA-256, HMAC).

- Применить изученные методы на конкретном примере передачи файлов между двумя системами.
- Проверить устойчивость разработанной системы к атакам модификации данных.
- Оформить отчет с описанием проведенных экспериментов и выводами относительно надежности методов контроля целостности.

Краткие методические указания

На выполнение одной практической работы отводится не менее одного двухчасового занятия. После выполнения каждой практической работы студент должен представить отчет о ее выполнении, а также, по указаниям преподавателя, выполнить дополнительные задания по теме

Шкала оценки

Оценка	Баллы	Описание
5	8-15	Оценка «отлично» выставляется, если студент выполнил задание, правильно применил методы.
4	5-7	Оценка «хорошо» выставляется, если студент выполнил задание, правильно применил методы, но совершил логические ошибки.
3	2-4	Оценка «удовлетворительно» выставляется, если студент выполнил задание, но применил методы не все необходимые методы для его выполнения.
2	0-1	Оценка «неудовлетворительно» выставляется в случае, если студент не выполнил задание и/ или неверно применил методы необходимые его выполнения.

5.3 Вопросы к экзамену

1. Определение информационной и компьютерной безопасности.
2. Классификация угроз информационной безопасности.
3. Определение и структура политики безопасности информационной системы.
4. Закрытые, открытые, гибридные политики информационной безопасности.
5. Аналитический метод описания политик безопасности.
6. Графовый метод описания политик безопасности.
7. Объектный метод описания политик безопасности.
8. Логический метод описания политик безопасности
9. Пример графового метода описания ПБ: визуальный язык объектных ограничений «Language on Objects for Security Constraints» (LaSCO).
10. Определение графа атак. Формальное описание построения модели графа атак.
11. Анализ графа атак. Модель злоумышленника.
12. Определение гарантированной (верифицируемой) защиты.
13. Методы обеспечения гарантированности защиты.
14. Каналы несанкционированного доступа, утечки информации и деструктивных воздействий на информационную среду (НСДУВ).
15. Вероятностная оценка реализации канала НСДУВ.
16. Формальное описание обобщённой модели системы защиты информационной системы.
17. Формальное описание вероятностной модели систем защиты информационной системы.
18. Формальное описание модели безопасности информационной системы, построенной с использованием теории графов.
19. Формальное описание модели безопасности информационной системы, построенной с использованием теории автоматов.
20. Основные понятия защиты информации (субъекты, объекты, доступ, граф доступов,

информационные потоки).

21. Модель системы безопасности HRU. Основные положения модели.

22. Теорема об алгоритмической неразрешимости проблемы безопасности в произвольной

системе HRU.

23. Модель типизированной матрицы доступов. Основные положения модели.

24. Теорема о существовании алгоритма проверки безопасности ациклических систем

монотонных ТМД.

25. Модель распространения прав доступа Take-Grant. Теоремы о передаче прав в графе доступов, состоящем из субъектов, и произвольном графе доступов.

26. Расширенная модель Take-Grant и ее применение для анализа информационных потоков

в автоматизированной системе (АС).

27. Модель Белла-Лападулы как основа построения систем мандатного разграничения доступа. Основные положения модели.

28. Базовая теорема безопасности (BST). Политика low-watermark в модели Белла-ЛаПадулы.

29. Применения модели Биба для реализации мандатной политики целостности.

30. Применение модели систем военных сообщений для систем приема, передачи и обработки почтовых сообщений, реализующих мандатную политику безопасности.

31. Шесть теоретических принципов политики контроля целостности. Соответствие правил модели Кларка-Вилсона принципам политики целостности.

32. Понятие ролевого управления доступом. Базовая модель ролевого управления доступом.

33. Понятие администрирования ролевого управления доступом. Администрирование

иерархии ролей.

34. Понятие мандатного ролевого управления доступом. Требования либерального мандатного управления доступом.

35. Автоматная модель безопасности информационных потоков.

36. Вероятностная модель безопасности информационных потоков.

37. Информационное невлияние. Информационное невлияние с учетом фактора времени.

38. Монитор безопасности объектов. Монитор безопасности субъектов.

39. Теоремы о достаточных условиях гарантированного выполнения политики безопасности в компьютерных системах.

Краткие методические указания

Для подготовки к экзамену студенту необходимо изучить лекционный материал, а так же материал представленный в дополнительных источниках.

Шкала оценки

Оценка	Баллы	Описание
5	14-20	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.
4	8-12	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.
3	2-6	Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки.
2	0-2	Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки.