

**МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ
И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ**

Северо-Кавказский филиал
ордена Трудового Красного Знамени федерального государственного
бюджетного образовательного учреждения высшего образования
«Московский технический университет связи и информатики»

Утверждаю
Зам. директора по УР
Н.А. Андреева
«31» 03 2025 г.

Рабочая программа дисциплины

Б1.О.30 Моделирование систем защиты информации

Кафедра: **Информационной безопасности**
Направление подготовки: **10.03.01 Информационная безопасность**
Профиль: **Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)**
Формы обучения: **очная**

Распределение часов дисциплины по семестрам (очная форма обучения (ОФО))

Вид учебной работы	ОФО	
	ЗЕ	часов/семестр
Общая трудоемкость дисциплины, в том числе (по семестрам, курсам):	5	180/7
Контактная работа, в том числе (по семестрам, курсам):		96/7
Лекции		36/7
Лабораторных работ		24/7
Практических занятий		36/7
Семинаров		
Самостоятельная работа		48/7
Контроль		36/7
Число контрольных работ (по курсам)		
Число КР (по семестрам, курсам)		
Число КП (по семестрам, курсам)		
Число зачетов с разбивкой по семестрам (курсам)		
Число экзаменов с разбивкой по семестрам (курсам)		1/7

Программу составил:
к.т.н. доцент Юхнов В.И.

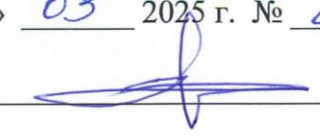
Рабочая программа дисциплины
«Моделирование систем защиты информации»

Разработана в соответствии с ФГОС ВО:
направления подготовки **10.03.01 «Информационная безопасность»**, утвержденным
приказом Министерства науки и высшего образования Российской Федерации от 17
ноября 2020 г. N 1427.

Составлена на основании учебного плана
направления **10.03.01 «Информационная безопасность»** профиля «Безопасность
компьютерных систем (по отрасли или в сфере профессиональной деятельности)»,
одобренного Учёным советом СКФ МТУСИ, протокол № 8 от 31.03.2025г., и
утвержденного директором СКФ МТУСИ 31.03.2025 г.

Рассмотрена и одобрена на заседании кафедры
Информационная безопасность

Протокол от «31» 03 2025 г. № 8

И.о. зав. кафедрой  А.Г.Жуковский

1. Цели изучения дисциплины

Целью освоения дисциплины является формирование у обучаемых знаний, умений и навыков, позволяющих применять современные методы моделирования систем защиты информации, интерпретирование полученных результатов для решения задач проектирования и прогнозирования качества работы компьютерных систем.

2. Планируемые результаты обучения

Изучение дисциплины направлено на формирование у обучающегося способности решать профессиональные задачи в соответствии с **эксплуатационным** видом деятельности:

Результатом освоения дисциплины являются сформированные у обучающегося следующие компетенции:

Компетенции, формируемые у обучающегося в результате освоения дисциплины (в части, обеспечиваемой дисциплиной)	
ОПК-11: Способен проводить эксперименты по заданной методике и обработку их результатов	
Знать:	
- основные понятия и определения, используемые при описании моделей безопасности КС; - виды политик управления доступом и информационными потоками в КС; - современные методы моделирования систем защиты информации.	
Уметь:	
- проводить эксперименты по заданным методикам и обработку их результатов; - использовать современные методы моделирования систем защиты информации; - применять комплексный подход к обеспечению информационной безопасности объекта защиты.	
Владеть:	
- навыками построения стандартных процедур принятия решений, на основе имеющихся экспериментальных данных; - практическими навыками применения политик управления доступом и информационными потоками в КС; - практическими навыками применения современных методов моделирования систем защиты информации.	

3. Место дисциплины в структуре образовательной программы

Требования к предварительной подготовке обучающегося (предшествующие дисциплины, модули, темы):	
1	Б1.О.14 Информационные технологии и программирование
2	Б1.О.32 Основы управления информационной безопасностью
3	Б1.О.36.03 Безопасность компьютерных сетей
Последующие дисциплины и практики, для которых освоение данной дисциплины необходимо:	
1	Б2.В.03(Пд) Производственная (преддипломная) практика
2	Б3.О.01 Подготовка к процедуре защиты и защита выпускной квалификационной работы

4. Структура и содержание дисциплины

4.1 Очная форма обучения, 4 года (всего 180 часов, 96 аудиторных часов, 84 часа самостоятельной работы)

Код зан.	Тема и краткое содержание занятия	Вид зан.	Кол. часов	Компетенции	УМИО
Курс 4, Семестр 7					
Модуль 1: Модели безопасности КС – 72 (48+24) часов					
1.1	Основные понятия и определения, используемые при описании моделей безопасности компьютерных систем	Лек1	2	ОПК-11	Л1.1
1.2	Модели компьютерных систем с дискреционным управлением доступом	Лек2	2	ОПК-11	Л1.1 Л2.1
1.3	Пр №1. Модель решетки.	ПЗ 1	6	ОПК-11	Л1.1 Л3.1
1.4	ЛР №1. Модель ХРУ и ТМД.	ЛР 1	6	ОПК-11	Л1.1 Л3.1
1.5	Модели компьютерных систем с мандатным управлением доступом	Лек3	2	ОПК-11	Л1.1 Л2.1
1.6	Модели компьютерных систем с ролевым управлением доступом	Лек4	4	ОПК-11	Л1.1 Л3.1
1.7	Модели безопасности информационных потоков	Лек5	4	ОПК-11	Л1.1 Л2.1 Л2.2
1.8	Модели безопасности управления доступом и информационными потоками	Лек6	4	ОПК-11	Л1.1 Л2.1 Л2.2
1.9	ЛР №2. Классическая модель Белла-ЛаПадулы и ее интерпретации	ЛР 2	6	ОПК-11	Л1.1 Л3.1
1.10	ЛР №3 Модели ролевого управления доступом.	ЛР 3	6	ОПК-11	Л1.1 Л3.1
1.11	ЛР №4 Модели безопасности информационных потоков.	ЛР 4	6	ОПК-11	Л1.1 Л3.1
1.12	Дискреционные ДП-модели. Модель СВС. МРОСЛ ДП-модель. Основные виды формальных моделей безопасности. Проблема адекватности реализации модели безопасности. Классическая модель Take-Grant. Расширенная модель Take-Grant.	СРС	24	ОПК-11	Л2.1 Л2.2
Модуль 2. Методы моделирования систем защиты информации – 72 (48+24) часов					
2.1	Проектирование системы защиты информации с использованием модели с полным перекрытием множества угроз	Лек7	2	ОПК-11	Л2.1 Л2.2 Л3.1
2.2	Модель безопасности с полным перекрытием множества угроз	ПЗ 2	6	ОПК-11	Л2.1
2.3	Анализ рисков информационной безопасности	Лек8	2	ОПК-11	Л2.1 Л2.2 Л3.1
2.4	Анализ рисков информационной безопасности с использованием методики COBIT	ПЗ 3	6	ОПК-11	Л2.1
2.5	Система поддержки принятия Парето-оптимальных решений в области проектирования системы защиты	Лек9	2	ОПК-11	Л2.1 Л2.2

	информации				ЛЗ.1
2.6	Метод принятия решений в разработке системы защиты информации на основе закона Парето и метода достижимых целей	ПЗ 4	6	ОПК-11	Л2.1
2.7	Анализ рисков информационной безопасности с использованием программного комплекса ГРИФ	СРС	8	ОПК-11	Л2.1
2.8	Моделирование на основе сети Петри	Лек10	4	ОПК-11	Л2.1 Л2.2 ЛЗ.1
2.9	Разработка сценариев действий нарушителя ИБ с использованием сети Петри	ПЗ 5	6	ОПК-11	Л2.1
2.10	Методологии и стандарты IDEF для моделирования процессов в защищенных системах обработки информации	Лек11	4	ОПК-11	Л2.1 Л2.2 ЛЗ.1
2.11	Использование методологии и стандарты IDEF для моделирования процессов в защищенных системах обработки информации	ПЗ 6	6	ОПК-11	Л2.1
2.12	Определение показателей защищенности информации при несанкционированном доступе. Методы расчета прочности оболочки защиты	СРС	8	ОПК-11	Л2.1 Л2.2
2.13	Анализ рисков ИБ для малого и среднего бизнеса. Матричный подход к анализу рисков информационной безопасности. Расчетная методика оценки рисков ИБ.	СРС	8	ОПК-11	Л2.1 Л2.2
2.14	Анализ и оценка рисков ИБ с использованием нечеткой логики. Построение оптимальной системы защиты информации.	Лек12	4	ОПК-11	Л1.1 ЛЗ.1
	Экзамен		36	ОПК-11	Л1.1 Л1.2 Л2.1 Л2.2 ЛЗ.1 ЛЗ.2
	Итого		180		

5. Учебно-методическое и информационное обеспечение дисциплины

5.1. Рекомендуемая литература				
5.1.1. Основная литература				
Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л1.1	Богульская, Н.А. М. М. Кучеров	Модели безопасности компьютерных систем : учебное пособие	Красноярск : Сиб. федер. ун-т, 2019. - 206 с. -	Э1
5.1.2. Дополнительная литература				
Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л2.1	Гришина, Н. В.	Основы моделирования процессов и систем защиты информации : учебное пособие	Москва : ИНФРА-М, 2022. — 107 с.	Э2
Л2.2	Черняков, М. К.	Моделирование и проектирование производственных процессов и систем : учебное пособие	Новосибирск : Изд-во НГТУ, 2020. - 94 с. -	Э3

5.1.3. Учебно-методическое обеспечение				
Код	Авторы, составители	Заглавие	Издательство, год	Кол.
ЛЗ.1	Е.К. Баранова, Бабаш, А. В.	Моделирование системы защиты информации. Практикум : учебное пособие	Москва : РИОР : ИНФРА-М, 2021. — 320 с.	Э4
5.2. Электронные образовательные ресурсы				
Э1	https://znanium.ru/catalog/document?id=380447			
Э2	https://znanium.com/catalog/product/1891122 .			
Э3	https://znanium.com/catalog/product/1866933 .			
Э4	https://znanium.ru/catalog/document?id=371348			
5.3 Информационно-справочные системы и профессиональные базы данных				
5.3.1	Консультант Плюс – https://www.consultant.ru/			
5.3.2	Гарант – https://www.garant.ru/			
5.3.2	Сборник нормативных документов «Регламент» – https://reglament.pro/index.php/entrance (неограниченный доступ для авторизованных пользователей)			
5.3.3	Научная электронная библиотека – https://www.elibrary.ru/			
5.3.4	Профессиональная база данных: Федеральный портал «Российское образование»: [Электронный ресурс] – Режим доступа: http://www.edu.ru/ (открытый доступ)			
5.3.5	Профессиональная база данных: Федеральный центр информационно-образовательных ресурсов: [Электронный ресурс] – Режим доступа: http://fcior.edu.ru/ (открытый доступ)			
5.3.6	Национальный открытый университет «ИНТУИТ» - https://intuit.ru/			
5.4. Программное обеспечение				
СКФ МТУСИ обеспечен необходимым комплектом лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства:				
П.1	Kaspersky Endpoint Security			
П.2	Операционная система Linux			
П.3	Пакет Microsoft Office лицензионное ПО			
П.4	ПО «Coras»			
П.5	Программный комплекс «RA2»			

6. Материально-техническое обеспечение дисциплины

6.1 МТО лекционных занятий	
1	Лекционная аудитория, оборудованная интерактивной доской, проектором
6.2 МТО лабораторных работ и практических занятий	
1	Учебные аудитории, оборудованные компьютерной техникой, с возможностью подключения к сети «Интернет», и обеспечением доступа в электронную информационно-образовательную среду СКФ МТУСИ
6.3 МТО рубежных контролей, экзамена	
1	Учебные аудитории, оборудованные компьютерной техникой с возможностью выхода в локальную сеть Филиала и Интернет.
6.4 МТО самостоятельной работы обучающихся	
1	Помещение для самостоятельной работы обучающихся оснащено компьютерной техникой с возможностью подключения к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду СКФ МТУСИ

7. Оценочные материалы

Оценочные материалы и перечень видов оценочных средств текущего контроля и промежуточной
--

аттестации представлены в Приложении 1 к рабочей программе дисциплины.
--

8. Методические рекомендации для обучающихся по освоению дисциплины
--

Методические рекомендации по освоению дисциплины представлены в Приложении 2 к рабочей программе дисциплины.
--

9. Особенности реализации дисциплины (модуля) при обучении инвалидов и лиц с ограниченными возможностями здоровья

Рабочая программа дисциплины (модуля) при необходимости может быть адаптирована для обучения (в том числе с применением дистанционных образовательных технологий) лиц с ограниченными возможностями здоровья, инвалидов. Для этого требуется заявление обучающихся, являющихся лицами с ограниченными возможностями здоровья, инвалидами, или их законных представителей и рекомендации психолого-медико-педагогической комиссии. При обучении лиц с ограниченными возможностями здоровья учитываются их индивидуальные психофизические особенности. Обучение инвалидов осуществляется также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).

Для лиц с нарушением слуха возможно предоставление учебной информации в визуальной форме (краткий конспект лекций; тексты заданий, напечатанные увеличенным шрифтом), на аудиторных занятиях допускается присутствие ассистента, а также сурдопереводчиков и тифлосурдопереводчиков.

Текущий контроль успеваемости осуществляется в письменной форме: обучающийся письменно отвечает на вопросы, письменно выполняет практические задания.

Доклад (реферат) также может быть представлен в письменной форме, при этом требования к содержанию остаются теми же, а требования к качеству изложения материала (понятность, качество речи, взаимодействие с аудиторией и т. д.) заменяются на соответствующие требования, предъявляемые к письменным работам (качество оформления текста и списка литературы, грамотность, наличие иллюстрационных материалов и т.д.).

Промежуточная аттестация для лиц с нарушениями слуха проводится в письменной форме, при этом используются общие критерии оценивания. При необходимости время подготовки к ответу может быть увеличено.

Для лиц с нарушением зрения допускается аудиальное предоставление информации, а также использование на аудиторных занятиях звукозаписывающих устройств (диктофонов и т.д.). Допускается присутствие на занятиях ассистента (помощника), оказывающего обучающимся необходимую техническую помощь.

Текущий контроль успеваемости осуществляется в устной форме.

При проведении промежуточной аттестации для лиц с нарушением зрения тестирование может быть заменено на устное собеседование по вопросам.

Для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, на аудиторных занятиях, а также при проведении процедур текущего контроля успеваемости и промежуточной аттестации могут быть предоставлены необходимые технические средства (персональный компьютер, ноутбук или другой гаджет); допускается присутствие ассистента (ассистентов), оказывающего обучающимся необходимую техническую помощь (занять рабочее место, передвигаться по аудитории, прочитать задание, оформить ответ, общаться с преподавателем).

10. Дополнения и изменения в Рабочей программе

Лист актуализации рабочей программы дисциплины «Моделирование систем защиты информации Б1.О.30» для использования в 20___/20___ учебном году

Утверждаю

Зам. директора по УР _____
«___» _____ 20___ г.

Направление: 10.03.01 Информационная безопасность

Профиль: Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)

Форма обучения: очная

(Возможны следующие варианты):

а) Рабочая программа действует без изменений.

б) В рабочую программу вносятся следующие изменения:

1)

2)

3)

Разработчик (и): _____

(ФИО, ученая степень, ученое звание)

«___» _____ 20___ г.

Рабочая программа пересмотрена и одобрена на заседании кафедры ИБ

Протокол № _____ от «___» _____ 20___ г.

Заведующий кафедрой _____

Оценочные материалы для проведения текущего контроля и промежуточной аттестации по дисциплине

1. Оценочные материалы для проведения промежуточной аттестации по дисциплине

1.1 Шкала оценивания компетенций

Шкала оценивания компетенций		
Оценка	Уровень освоения компетенции	Критерии оценивания
«Отлично»	Высокий уровень	Обучающийся показывает всестороннее, систематическое и глубокое знание основного и дополнительного учебного материала, умеет свободно выполнять задания, предусмотренные программой; усвоил основную и знаком с дополнительной рекомендованной литературой; может объяснить взаимосвязь основных понятий дисциплины в их значении для последующей профессиональной деятельности; проявляет творческие способности в понимании, изложении и использовании учебного материала.
«Хорошо»	Повышенный уровень	Обучающийся показывает достаточный уровень знаний в пределах основного учебного материала, без существенных ошибок выполняет предусмотренные в программе задания; усвоил основную литературу, рекомендованную в программе; способен объяснить взаимосвязь основных понятий дисциплины при дополнительных вопросах преподавателя. Допускает не существенные погрешности в ответах, устраняет их без помощи преподавателя.
«Удовлетворительно»	Пороговый уровень	Обучающийся показывает знания основного учебного материала в минимальном объеме, необходимом для дальнейшей учебы; справляется с выполнением заданий, предусмотренных программой, допуская при этом большое количество не принципиальных ошибок; знаком с основной литературой, рекомендованной программой. Допускает существенные погрешности в ответах, но обладает необходимыми знаниями для их устранения под руководством преподавателя.
«Неудовлетворительно»	Минимальный уровень не достигнут	Обучающийся обнаруживает пробелы в знаниях основного учебного материала, допускает принципиальные ошибки в выполнении предусмотренных программой заданий, не знаком с рекомендованной литературой, не может исправить допущенные ошибки. Как

		правило, оценка «неудовлетворительно» ставится обучающимся, которые не могут продолжить обучение или приступить к профессиональной деятельности по окончании вуза без дополнительных занятий по соответствующей дисциплине.
--	--	---

1.2 Показатели, критерии и шкалы оценивания компетенций

Показатели компетенции	Критерии оценивания	Шкала оценивания
ОПК-11: Способен проводить эксперименты по заданной методике и обработку их результатов		
Знать:		
- основные понятия и определения, используемые при описании моделей безопасности КС; - виды политик управления доступом и информационными потоками в КС;	Контрольная работа	Модуль 1 0÷13 «Неудовлетворительно» - 0-4 «Удовлетворительно» - 5-7 «Хорошо» - 8-10 «Отлично» - 10-13
- современные методы моделирования систем защиты информации.	Контрольная работа	Модуль 2 0÷12 «Неудовлетворительно» - 0-4 «Удовлетворительно» - 5-7 «Хорошо» - 7-10 «Отлично» - 10-12
Уметь:		
- проводить эксперименты по заданным методикам и обработку их результатов;	Практическое занятие 1	Модуль 1 0÷5 «Неудовлетворительно» - 0-1 «Удовлетворительно» - 2-3 «Хорошо» - 3-4 «Отлично» - 4-5
- использовать современные методы моделирования систем защиты информации; - применять комплексный подход к обеспечению информационной безопасности объекта защиты.	Практическое занятие 2	Модуль 2 ÷5 «Неудовлетворительно» - 0-1 «Удовлетворительно» - 2-3 «Хорошо» - 3-4 «Отлично» - 4-5
Владеть:		
- навыками построения стандартных процедур принятия решений на основе имеющихся экспериментальных данных, - навыками моделирования систем безопасности с полным перекрытием множества угроз; - навыками использования стандартов и методологий анализа экспериментальных данных	Лабораторная работа 2	Модуль 1 0÷5 «Неудовлетворительно» - 0-1 «Удовлетворительно» - 2-3 «Хорошо» - 3-4 «Отлично» - 4-5
- навыками построения стандартных процедур принятия решений, на	Лабораторная работа 3	Модуль 1 0÷5 «Неудовлетворительно» - 0-1

основе имеющихся экспериментальных данных		«Удовлетворительно» - 2-3 «Хорошо» - 3-4 «Отлично» - 4-5
- практическими навыками применения политик управления доступом и информационными потоками в КС; - практическими навыками применения современных методов моделирования систем защиты информации	Практическое занятие 3	Модуль 2 0÷5 «Неудовлетворительно» - 0-1 «Удовлетворительно» - 2-3 «Хорошо» - 3-4 «Отлично» - 4-5
	Экзамен	0-100 «Неудовлетворительно» - 0-40 «Удовлетворительно» - 41-60 «Хорошо» - 61-80 «Отлично» - 81-100

1.3 Оценочные материалы: типовые контрольные задания, иные материалы

1.3.1 Оценочные материалы для текущего контроля для очной формы обучения

Модуль 1 (50 баллов):

Модуль содержит 6 лекционных занятий, 1 практическое занятие и 4 лабораторных работы. Знание лекционного материала оценивается по контрольной работе, состоящей из двух вопросов, максимальное количество баллов за контрольную работу составляет 25. За каждое выполненное и защищенное лабораторное и практическое занятия обучающийся получает максимум 5 баллов. За практическое занятие и лабораторные работы обучающийся получает максимум 25 баллов. Общее максимальное количество баллов за модуль 1 составляет 50.

Вопросы для контрольной работы (ОПК-11):

1. В чем состоит важность основной аксиомы теории информационной безопасности в рамках субъект-сущностного подхода?
2. Какие основные угрозы безопасности информации рассматриваются в теории информационной безопасности?
3. Приведите примеры наиболее распространенных в современных ОС и СУБД запрещенных информационных потоков по памяти и по времени.
4. Какие основные виды политик управления доступом рассматриваются в теории информационной безопасности?
5. В чем состоит основная проблема реализации модели безопасности в КС?
6. Для команды $C(qi0, Ai0) = (qi1, Ai1, l)$ машины Тьюринга выпишите две представляющие её команды модели ХРУ.
7. Докажите, что для общего случая систем ХРУ не существует алгоритма проверки возможности утечки права доступа r для заданной пары субъект s и объект o .
8. Представьте произвольную систему ТМД системой ХРУ.
9. Выразите правило sru расширенной модели Take-Grant через её другие де-факто правила.
10. Как по аналогии с определением безопасного начального состояния в модели ХРУ и с использованием определения предиката $can_share(a, x, y, G0)$ определить безопасное начальное состояние в модели Take-Grant?

11. Как представить систему, построенную на основе расширенной модели Take-Grant, системами ХРУ и ТМД?
12. Каковы основные недостатки классической модели Белла-ЛаПадулы?
13. Как сформулировать теорему БТБ для модели мандатной политики целостности информации Биба?
14. Известно, что при реализации мандатного управления доступом может допускаться использование правил дискреционного управления доступом (например, с использованием ds- свойства безопасности модели Белла-ЛаПадулы). Учитывая это обстоятельство, предложите подход по созданию запрещенного информационного потока от объекта с высоким уровнем конфиденциальности к объекту с низким уровнем конфиденциальности, использующий кооперацию субъектов КС.
15. Каким образом десять неформальных свойств модели СВС реализуются в её формальном описании?
16. Где в определениях безопасности модели СВС реализованы свойства безопасности (ss-свойство, *- свойство и ds-свойство) классической модели Белла-ЛаПадулы?
17. Какие основные проблемы определения правил изменения иерархий ролей рассматриваются в модели администрирования ролевого управления доступом?
18. Какого вида ограничения, описанные в базовой модели ролевого управления доступом, могут быть использованы при определении требований либерального и строгого мандатного управления доступом?
19. Каким образом в определениях либерального или строгого мандатного управления доступом модели ролевого управления доступом реализованы ss-свойство и *- свойство, определенные в классической модели Белла-ЛаПадулы?
20. В чем состоит развитие в моделях атрибутивного управления доступом подходов, использованных при формировании моделей ролевого управления доступом семейства RBAC?
21. Опишите средствами базовой модели атрибутивного управления доступом свойства безопасности для доступов, изложенные в классической модели Белла-ЛаПадулы, а также в ее интерпретации «Безопасность переходов»
22. Каковы основные функции МБО и МБС в ИПС, в чем их отличие друг от друга?
23. Почему для реализации ИПС необходимо требовать наличия в КС контроля порождения субъектов?
24. В чем отличие структуры ядра безопасности в классических моделях безопасности КС от структуры ядра безопасности в субъектно-ориентированной модели ИПС?
25. Какой вид политики управления доступом используется в качестве основы автоматной модели безопасности информационных потоков?
26. Почему использование определения требований информационного невливания (с учетом времени) позволяет обеспечить возможность функционирования в КС монитора ссылок и системы аудита?

Практическое занятие 1. Модель решетки.

Контрольные вопросы Пр№1 (ОПК-11):

1. В чем состоит важность основной аксиомы теории информационной безопасности в рамках субъект-сущностного подхода?
2. Какие основные угрозы безопасности информации рассматриваются в теории информационной безопасности?
3. Приведите примеры наиболее распространенных в современных ОС и СУБД запрещенных информационных потоков по памяти и по времени.
4. Какие основные виды политик управления доступом рассматриваются в теории информационной безопасности?
5. В чем состоит основная проблема реализации модели безопасности в КС?
6. Решение задач.

Лабораторная работа №1. Модель Харрисона-Руззо-Ульмана и ТМД.

Контрольные вопросы ЛР№1 :

1. Для команды $C(qi_0, Ai_0) = (qi_1, Ai_1, l)$ машины Тьюринга выпишите две представляющие её команды модели ХРУ.
2. Докажите, что для общего случая систем ХРУ не существует алгоритма проверки возможности утечки права доступа g для заданной пары субъект s и объект o .
3. Представьте произвольную систему ТМД системой ХРУ.
4. Выразите правило spy расширенной модели *Take-Grant* через её другие де-факто правила.
5. Как по аналогии с определением безопасного начального состояния в модели ХРУ и с использованием определения предиката $can_share(a, x, y, G_0)$ определить безопасное начальное состояние в модели *Take-Grant*?
6. Как представить систему, построенную на основе расширенной модели *Take-Grant*, системами ХРУ и ТМД?

Лабораторная работа №2. Классическая модель Белла-ЛаПадулы и ее интерпретации

Контрольные вопросы ЛР№1 (ОПК-11):

1. Каковы основные недостатки классической модели Белла-ЛаПадулы?
2. Как сформулировать теорему БТБ для модели мандатной политики целостности информации Биба?
3. Известно, что при реализации мандатного управления доступом может допускаться использование правил дискреционного управления доступом (например, с использованием *ds*-свойства безопасности модели Белла-ЛаПадулы). Учитывая это обстоятельство, предложите подход по созданию запрещенного информационного потока от объекта с высоким уровнем конфиденциальности к объекту с низким уровнем конфиденциальности, использующий кооперацию субъектов КС.
4. Каким образом десять неформальных свойств модели СВС реализуются в её формальном описании?
5. Где в определениях безопасности модели СВС реализованы свойства безопасности (*ss*-свойство, ***- свойство и *ds*-свойство) классической модели Белла-ЛаПадулы?

Лабораторная работа №3. Модели ролевого управления доступом

Контрольные вопросы ЛР№1 (ОПК-11):

1. Какие основные проблемы определения правил изменения иерархий ролей рассматриваются в модели администрирования ролевого управления доступом?
2. Какого вида ограничения, описанные в базовой модели ролевого управления доступом, могут быть использованы при определении требований либерального и строгого мандатного управления доступом?
3. Каким образом в определениях либерального или строгого мандатного управления доступом модели ролевого управления доступом реализованы *ss*-свойство и ***- свойство, определенные в классической модели Белла-ЛаПадулы?
4. В чем состоит развитие в моделях атрибутивного управления доступом подходов, использованных при формировании моделей ролевого управления доступом семейства RBAC?
5. Опишите средствами базовой модели атрибутивного управления доступом свойства безопасности для доступов, изложенные в классической модели Белла-ЛаПадулы, а также в ее интерпретации «Безопасность переходов»

Лабораторная работа №4. Модели безопасности информационных потоков.

Контрольные вопросы ЛР№1:

1. Каковы основные функции МБО и МБС в ИПС, в чем их отличие друг от друга?
2. Почему для реализации ИПС необходимо требовать наличия в КС контроля порождения

субъектов?

3. В чем отличие структуры ядра безопасности в классических моделях безопасности КС от структуры ядра безопасности в субъектно-ориентированной модели ИПС?
4. Какой вид политики управления доступом используется в качестве основы автоматной модели безопасности информационных потоков?
5. Почему использование определения требований информационного невливания (с учетом времени) позволяет обеспечить возможность функционирования в КС монитора ссылок и системы аудита?

Модуль 2 (50 баллов):

Модуль содержит 6 лекционных занятий и 5 практических занятий. Знание лекционного материала оценивается по контрольной работе, состоящей из двух вопросов, максимальное количество баллов за контрольную работу составляет 25. За каждое выполненное и защищенное практическое занятия обучающийся получает максимум 5 баллов. Общее максимальное количество баллов за модуль 1 составляет 50.

Вопросы для контрольной работы (ОПК-11):

1. Какие методы моделирования наиболее эффективны при построении системы защиты объекта информатизации?
2. Опишите этапы построения модели с полным перекрытием множества угроз безопасности.
3. В чем особенность, достоинства и недостатки модели с полным перекрытием множества угроз безопасности?
4. Для каких объектов оценки модель с полным перекрытием множества угроз не может применяться? Приведите аргументацию и конкретные примеры.
5. Какие выводы могут быть сформулированы на основе анализа двудольного графа модели с полным перекрытием множества угроз? Приведите конкретный пример.
6. Какие выводы могут быть сформулированы на основе анализа трехдольного графа модели с полным перекрытием множества угроз? Приведите конкретный пример.
7. На каких этапах создания защищенных информационных систем рекомендуется использование модели с полным перекрытием множества угроз?
8. Какими методами оценки экономической эффективности системы защиты объекта информатизации можно дополнить анализ трехдольного графа?
9. Как осуществляется декомпозиция общей задачи оценки эффективности функционирования системы защиты? Приведите пример модели элементарной защиты объекта информатизации и расчета прочности оболочки защиты.
10. Приведите пример модели многозвенной защиты объекта информатизации. Как в этом случае рассчитывается прочность защиты?
11. Какая информация должна быть собрана на объекте оценки для проведения анализа информационных рисков?
12. В каких единицах измеряется риск?
13. Выберите оптимальную стратегию управления рисками в следующем случае: веб-сервер компании находится внутри корпоративной сети и его программное обеспечение, возможно, содержит уязвимости.
14. Какую информацию необходимо получить на объекте оценки для определения ущерба по угрозе «нарушение целостности информации»?
15. Какую информацию необходимо получить на объекте оценки для определения ущерба по угрозе «нарушение конфиденциальности информации»?

16. В случае анализа рисков ИС на базовом уровне какими стандартами в области защиты информации необходимо руководствоваться?
17. В случае полного анализа рисков ИС какие подходы обычно используются на практике?
18. Какие этапы должен включать аудит информационной безопасности?
19. Как осуществляется анализ информационных рисков, угрозы и уязвимости системы по двум факторам?
20. Как осуществляется анализ информационных рисков, угрозы и уязвимости системы по трем факторам?
21. Какие требования предъявляются к набору критериев для оценки альтернативных решений?
22. Как оценивается важность критериев?
23. Приведите классификацию задач принятия решений в области проектирования СЗИ.
24. Назовите основные этапы принятия управленческих решений в области построения защищенных систем обработки информации.
25. Приведите пример генерирования множества альтернатив с применением экспертных методов при разработке СЗИ.
26. Приведите пример использования метода строчных сумм для составления матрицы альтернативных проектов СЗИ.
27. Сформулируйте принцип Парето. В чем достоинства и недостатки его практического применения для принятия управленческих решений в области построения защищенных систем обработки информации?
28. Что понимается под паретооптимальным множеством?
29. Какие дополнительные возможности предоставляет метод достижимых целей для принятия управленческих решений в области построения защищенных систем обработки информации?
30. Опишите последовательность шагов при использовании паретооптимизации в выборе альтернативных проектов СЗИ.
31. В чем отличие сетей Петри от других способов моделирования в системах защиты информации?
32. Каким образом можно интерпретировать позиции и переходы при разработке сценариев действия нарушителя на объекте информатизации с использованием сети Петри? Приведите конкретные примеры.
33. В чем заключается ограниченность использования сетей Петри для моделирования процессов, происходящих в ИС?
34. Каким образом можно интерпретировать использование маркеров в сети Петри при моделировании действий нарушителя? Приведите конкретные примеры.
35. Какие выводы можно сделать о достижимости конечной цели атак при запуске разработанной сети Петри?

Практическое занятие 2. Модель безопасности с полным перекрытием множества угроз.

Контрольные вопросы Пр.№1 (ОПК-11):

1. Какие методы моделирования наиболее эффективны при построении системы защиты объекта информатизации?
2. Опишите этапы построения модели с полным перекрытием множества угроз безопасности.
3. В чем особенность, достоинства и недостатки модели с полным перекрытием множества угроз безопасности?
4. Для каких объектов оценки модель с полным перекрытием множества угроз не может применяться? Приведите аргументацию и конкретные примеры.
5. Какие выводы могут быть сформулированы на основе анализа двудольного графа модели с полным перекрытием множества угроз? Приведите конкретный пример.
6. Какие выводы могут быть сформулированы на основе анализа трехдольного графа модели с полным перекрытием множества угроз? Приведите конкретный пример.
7. На каких этапах создания защищенных информационных систем рекомендуется

использование модели с полным перекрытием множества угроз?

8. Какими методами оценки экономической эффективности системы защиты объекта информатизации можно дополнить анализ трехдольного графа?
9. Как осуществляется декомпозиция общей задачи оценки эффективности функционирования системы защиты? Приведите пример модели элементарной защиты объекта информатизации и расчета прочности оболочки защиты.
10. Приведите пример модели многозвенной защиты объекта информатизации. Как в этом случае рассчитывается прочность защиты?

Практическое занятие 3. Анализ рисков информационной безопасности с использованием методики COBIT

Контрольные вопросы Пр№1 (ОПК-11):

1. Какая информация должна быть собрана на объекте оценки для проведения анализа информационных рисков?
2. В каких единицах измеряется риск?
3. Выберите оптимальную стратегию управления рисками в следующем случае: веб-сервер компании находится внутри корпоративной сети и его программное обеспечение, возможно, содержит уязвимости.
4. Какую информацию необходимо получить на объекте оценки для определения ущерба по угрозе «нарушение целостности информации»?
5. Какую информацию необходимо получить на объекте оценки для определения ущерба по угрозе «нарушение конфиденциальности информации»?
6. В случае анализа рисков ИС на базовом уровне какими стандартами в области защиты информации необходимо руководствоваться?
7. В случае полного анализа рисков ИС какие подходы обычно используются на практике?
8. Какие этапы должен включать аудит информационной безопасности?
9. Как осуществляется анализ информационных рисков, угрозы и уязвимости системы по двум факторам?
10. Как осуществляется анализ информационных рисков, угрозы и уязвимости системы по трем факторам?

Практическое занятие 4. Метод принятия решений в разработке системы защиты информации на основе закона Парето и метода достижимых целей

Контрольные вопросы Пр№1:

1. Какие требования предъявляются к набору критериев для оценки альтернативных решений?
2. Как оценивается важность критериев?
3. Приведите классификацию задач принятия решений в области проектирования СЗИ.
4. Назовите основные этапы принятия управленческих решений в области построения защищенных систем обработки информации.
5. Приведите пример генерирования множества альтернатив с применением экспертных методов при разработке СЗИ.
6. Приведите пример использования метода строчных сумм для составления матрицы альтернативных проектов СЗИ.
7. Сформулируйте принцип Парето. В чем достоинства и недостатки его практического применения для принятия управленческих решений в области построения защищенных систем обработки информации?
8. Что понимается под паретооптимальным множеством?
9. Какие дополнительные возможности предоставляет метод достижимых целей для принятия управленческих решений в области построения защищенных систем обработки информации?
10. Опишите последовательность шагов при использовании паретооптимизации в выборе альтернативных проектов СЗИ.

Практическое занятие 5. Разработка сценариев действий нарушителя ИБ с использованием сети Петри

Контрольные вопросы Пр.№1:

1. В чем отличие сетей Петри от других способов моделирования в системах защиты информации?
2. Каким образом можно интерпретировать позиции и переходы при разработке сценариев действия нарушителя на объекте информатизации с использованием сети Петри? Приведите конкретные примеры.
3. В чем заключается ограниченность использования сетей Петри для моделирования процессов, происходящих в ИС?
4. Каким образом можно интерпретировать использование маркеров в сети Петри при моделировании действий нарушителя? Приведите конкретные примеры.
5. Какие выводы можно сделать о достижимости конечной цели атак при запуске разработанной сети Петри?

1.3.2. Вопросы, выносимые на экзамен по дисциплине «Моделирование систем защиты информации» (ОПК-11) (промежуточная аттестация):

1. В чем состоит важность основной аксиомы теории информационной безопасности в рамках субъект-сущностного подхода?
2. Какие основные угрозы безопасности информации рассматриваются в теории информационной безопасности?
3. Приведите примеры наиболее распространенных в современных ОС и СУБД запрещенных информационных потоков по памяти и по времени.
4. Какие основные виды политик управления доступом рассматриваются в теории информационной безопасности?
5. В чем состоит основная проблема реализации модели безопасности в КС?
6. Для команды $C(qi0, Ai0) = (qi1, Ai1, l)$ машины Тьюринга выпишите две представляющие её команды модели ХРУ.
7. Докажите, что для общего случая систем ХРУ не существует алгоритма проверки возможности утечки права доступа r для заданной пары субъект s и объект o .
8. Представьте произвольную систему ТМД системой ХРУ.
9. Выразите правило sru расширенной модели Take-Grant через её другие де-факто правила.
10. Как по аналогии с определением безопасного начального состояния в модели ХРУ и с использованием определения предиката $can_share(a, x, y, G0)$ определить безопасное начальное состояние в модели Take-Grant?
11. Как представить систему, построенную на основе расширенной модели Take-Grant, системами ХРУ и ТМД?
12. Каковы основные недостатки классической модели Белла-ЛаПадулы?
13. Как сформулировать теорему БТБ для модели мандатной политики целостности информации Биба?
14. Известно, что при реализации мандатного управления доступом может допускаться использование правил дискреционного управления доступом (например, с использованием ds -свойства безопасности модели Белла-ЛаПадулы). Учитывая это обстоятельство, предложите подход по созданию запрещенного информационного потока от объекта с высоким уровнем конфиденциальности к объекту с низким уровнем конфиденциальности, использующий кооперацию субъектов КС.
15. Каким образом десять неформальных свойств модели СВС реализуются в её формальном описании?

16. Где в определениях безопасности модели СВС реализованы свойства безопасности (ss-свойство, *- свойство и ds-свойство) классической модели Белла-ЛаПадулы?
17. Какие основные проблемы определения правил изменения иерархий ролей рассматриваются в модели администрирования ролевого управления доступом?
18. Какого вида ограничения, описанные в базовой модели ролевого управления доступом, могут быть использованы при определении требований либерального и строгого мандатного управления доступом?
19. Каким образом в определениях либерального или строгого мандатного управления доступом модели ролевого управления доступом реализованы ss-свойство и *- свойство, определенные в классической модели Белла-ЛаПадулы?
20. В чем состоит развитие в моделях атрибутивного управления доступом подходов, использованных при формировании моделей ролевого управления доступом семейства RBAC?
21. Опишите средствами базовой модели атрибутивного управления доступом свойства безопасности для доступов, изложенные в классической модели Белла-ЛаПадулы, а также в ее интерпретации «Безопасность переходов»
22. Каковы основные функции МБО и МБС в ИПС, в чем их отличие друг от друга?
23. Почему для реализации ИПС необходимо требовать наличия в КС контроля порождения субъектов?
24. В чем отличие структуры ядра безопасности в классических моделях безопасности КС от структуры ядра безопасности в субъектно-ориентированной модели ИПС?
25. Какой вид политики управления доступом используется в качестве основы автоматной модели безопасности информационных потоков?
26. Почему использование определения требований информационного невливания (с учетом времени) позволяет обеспечить возможность функционирования в КС монитора ссылок и системы аудита?
27. Какие методы моделирования наиболее эффективны при построении системы защиты объекта информатизации?
28. Опишите этапы построения модели с полным перекрытием множества угроз безопасности.
29. В чем особенность, достоинства и недостатки модели с полным перекрытием множества угроз безопасности?
30. Для каких объектов оценки модель с полным перекрытием множества угроз не может применяться? Приведите аргументацию и конкретные примеры.
31. Какие выводы могут быть сформулированы на основе анализа двудольного графа модели с полным перекрытием множества угроз? Приведите конкретный пример.
32. Какие выводы могут быть сформулированы на основе анализа трехдольного графа модели с полным перекрытием множества угроз? Приведите конкретный пример.
33. На каких этапах создания защищенных информационных систем рекомендуется использование модели с полным перекрытием множества угроз?
34. Какими методами оценки экономической эффективности системы защиты объекта информатизации можно дополнить анализ трехдольного графа?
35. Как осуществляется декомпозиция общей задачи оценки эффективности функционирования системы защиты? Приведите пример модели элементарной защиты объекта информатизации и расчета прочности оболочки защиты.
36. Приведите пример модели многозвенной защиты объекта информатизации. Как в этом случае рассчитывается прочность защиты?
37. Какая информация должна быть собрана на объекте оценки для проведения анализа информационных рисков?
38. В каких единицах измеряется риск?
39. Выберите оптимальную стратегию управления рисками в следующем случае: веб-сервер компании находится внутри корпоративной сети и его программное обеспечение, возможно, содержит уязвимости.

40. Какую информацию необходимо получить на объекте оценки для определения ущерба по угрозе «нарушение целостности информации»?
41. Какую информацию необходимо получить на объекте оценки для определения ущерба по угрозе «нарушение конфиденциальности информации»?
42. В случае анализа рисков ИС на базовом уровне какими стандартами в области защиты информации необходимо руководствоваться?
43. В случае полного анализа рисков ИС какие подходы обычно используются на практике?
44. Какие этапы должен включать аудит информационной безопасности?
45. Как осуществляется анализ информационных рисков, угрозы и уязвимости системы по двум факторам?
46. Как осуществляется анализ информационных рисков, угрозы и уязвимости системы по трем факторам?
47. Какие требования предъявляются к набору критериев для оценки альтернативных решений?
48. Как оценивается важность критериев?
49. Приведите классификацию задач принятия решений в области проектирования СЗИ.
50. Назовите основные этапы принятия управленческих решений в области построения защищенных систем обработки информации.
51. Приведите пример генерирования множества альтернатив с применением экспертных методов при разработке СЗИ.
52. Приведите пример использования метода строчных сумм для составления матрицы альтернативных проектов СЗИ.
53. Сформулируйте принцип Парето. В чем достоинства и недостатки его практического применения для принятия управленческих решений в области построения защищенных систем обработки информации?
54. Что понимается под паретооптимальным множеством?
55. Какие дополнительные возможности предоставляет метод достижимых целей для принятия управленческих решений в области построения защищенных систем обработки информации?
56. Опишите последовательность шагов при использовании паретооптимизации в выборе альтернативных проектов СЗИ.
57. В чем отличие сетей Петри от других способов моделирования в системах защиты информации?
58. Каким образом можно интерпретировать позиции и переходы при разработке сценариев действия нарушителя на объекте информатизации с использованием сети Петри? Приведите конкретные примеры.
59. В чем заключается ограниченность использования сетей Петри для моделирования процессов, происходящих в ИС?
60. Каким образом можно интерпретировать использование маркеров в сети Петри при моделировании действий нарушителя? Приведите конкретные примеры.
61. Какие выводы можно сделать о достижимости конечной цели атак при запуске разработанной сети Петри?

2. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Порядок и методика проведения текущего контроля и промежуточной аттестации

Предусмотрены следующие виды контроля:

- текущий контроль по каждому модулю – в форме написания контрольной работы для оценки теоретических знаний;
- текущий контроль по каждому модулю – в форме отчетов по лабораторным работам и практическим занятиям для оценки практических навыков;
- промежуточная аттестация по дисциплине – в форме экзамена.

Текущий контроль успеваемости в форме защиты лабораторных и практических проводится в два этапа:

- 1-й этап: допуск к выполнению лабораторной работы – проводится в форме письменной «летучки» (5-10 мин) с целью контроля знаний обучающихся теоретической части лабораторной работы и готовности к выполнению практических исследований;

- 2-й этап выполняется по окончании каждой лабораторной работы (практического занятия) в форме индивидуального собеседования по выполненным исследованиям или расчетам. Проводится с целью контроля закрепления теоретической части материала и степени отработки обучающимся практических навыков исследования на аппаратуре.

Контрольные работы выполняются в виде короткого письменного ответа на один вопрос, изученный на предыдущей лекции в начале каждой последующей лекции. Ответ на вопрос дается в течение 5-10 минут. Таким образом, после лекционного курса каждого модуля формируется общая оценка за теоретические знания.

С целью повышения качества обучения за счет побуждения обучающихся к активной текущей учебной работе, четкого и оперативного контроля всего хода учебного процесса, снижения роли случайных и субъективных факторов при оценивании учебной деятельности обучающихся в образовательном процессе реализована модульно-рейтинговая система.

Правила ее использования прописаны в «Положении об МРС».

Набранные обучающимися баллы могут быть переведены в оценку:

- «неудовлетворительно» - от 0 до 40 от максимального количества баллов;
- «удовлетворительно» - от 41 до 60 максимального количества баллов;
- «хорошо» - от 61 до 80 максимального количества баллов;
- «отлично» - от 81 до 100 максимального количества баллов.

Соотношения максимального количества баллов, полученных обучающимися по блокам модулей, показаны в Таблице 1.

Таблица 1 - Распределение баллов по модулям дисциплины «Моделирование систем защиты информации»

Модуль	Всего баллов (Максимальное значение)	Теоретический блок (Контрольная работа)	Практический блок
Модуль 1	50	25	25=5+5+5+5+5
Модуль 2	50	25	25=5+5+5+5+5
Экзамен	100		

Теоретический блок оценивается по результатам контрольной работы. Практический блок оценивается по результатам выполнения лабораторных работ и заданий на практических занятиях.

На экзамене производится оценка тех компетенций, которые должны быть в той или иной форме освоены в процессе изучения. Рекомендуются формировать вопросы в экзаменационных билетах таким образом, чтобы преподаватель смог оценить все компетенции данной дисциплины.

3. Промежуточная аттестация

Промежуточная аттестация проводится в форме экзамена. Экзамен проводится по расписанию промежуточной аттестации в устном виде по экзаменационным билетам. Результаты аттестации заносятся в ведомость и зачетную книжку обучающегося.

Образец экзаменационного билета

	МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»	Утверждаю Зав. кафедрой «ИБ» _____ Жуковский А.Г. «___» _____ 20__ г.
Направление подготовки: 10.03.01 Информационная безопасность Курсы: 4 Дисциплина: Моделирование систем защиты информации		
Билет №1 1. В чем состоит важность основной аксиомы теории информационной безопасности в рамках субъект-сущностного подхода? 2. Какой вид политики управления доступом используется в качестве основы автоматной модели безопасности информационных потоков? «___» _____ 20__ г. Доцент, к.т.н. _____ Юхнов В.И		

Один комплект отпечатанных экзаменационных билетов, подписанных преподавателем кафедры и утвержденных заведующим кафедрой хранится у заведующего кафедрой, другой комплект – у преподавателя, ведущего дисциплину.

4. Тестовые задания по дисциплине «Моделирование систем защиты информации»

Тестовые задания позволяют оценить уровень сформированности компетенции ОПК-11
Задания распределены по блокам в соответствии с уровнем сложности. Каждый блок содержит номер задания, и текст задания.

Базовый уровень содержит примерно 50 % заданий.

Он формируется из заданий с выбором одного или нескольких верных ответов из предложенных или воспроизведения фактического материала (терминология, факты, классификация, параметры и др.);

Повышенный уровень в среднем составляет 35 % заданий.

В нем используются задания на сопоставление, сравнение, установление последовательности;

Высокий уровень в среднем составляют – 15 % заданий.

В задании используются: решения нетиповых задач, алгоритмы, доказательства, задания с развернутым ответом – определения, перечисление, изображение схемы, структуры и др.

Количество заданий по каждой компетенции равно 20. Всего 40 заданий.

Ключи к ответам представлены в отдельной таблице.

ОПК-11

Способен проводить эксперименты по заданной методике и обработку их результатов

БЛОК А (базовый уровень) – Задание с выбором одного или нескольких верных ответов из предложенных

Инструкция по тестам Блока А: Прочитайте текст и выберите один или несколько правильных ответов

№ задания	Тексты заданий
1	Цель экспериментального моделирования в курсе — это прежде всего: 1. Подбор «красивых» графиков. 2. Проверка гипотез и моделей защиты на данных по заранее заданной методике. 3. Увеличение объема отчёта. 4. Замена нормативных требований.
2	Что обязательно фиксировать в разделе «Методика» лабораторной работы? 1. Исходные данные/настройки и порядок шагов 2. Метрики/критерии оценки результата. 3. Только итоговый вывод. 4. Только фамилии исполнителей.
3	Какой принцип является ключевым для Bell–LaPadula? 1. Нет записи вверх. 2. Нет чтения вниз. 3. Нет чтения вверх. 4. Свободная передача прав.
4	Для модели Biba корректная формулировка: 1. Защищает конфиденциальность («нет чтения вверх») 2. О целостности: «нет записи вверх». 3. О доступности ресурсов. 4. Только ролевая иерархия.
5	Что является артефактами, повышающими воспроизводимость результатов? 1. Прикреплённые файлы проектов/скриптов. 2. Описание версий ПО и среды. 3. Ручное редактирование чисел в PDF. 4. Скрытие исходных данных.
6	В задании по RBAC уместно собирать: 1. Матрицу ролей и разрешений. 2. Журнал аудита попыток доступа.

№ задания	Тексты заданий
	3. Список MAC-адресов коммутатора. 4. Таблицу маршрутизации
7	В модели Take-Grant анализируют: 1. Распространение прав между субъектами и объектами. 2. Маршрутизацию по OSPF. 3. Шифрование TLS. 4. Балансировку нагрузки.
8	Что относится к моделям информационных потоков? 1. Контроль разрешённых направлений потоков. 2. Выявление побочных (covert) каналов. 3. Роуминг Wi-Fi. 4. Политика смены паролей.
9	Какое утверждение корректно для сетей Петри в контексте курса? 1. Используются только для графиков Ганта. 2. Описывают событийно-параллельные процессы (места, переходы, маркеры). 3. Это язык запросов к БД. 4. Только для моделирования TCP-стеков.
10	При анализе рисков целесообразно: 1. Оценивать вероятность и ущерб (ожидаемые потери). 2. Сопоставлять результаты со сценариями/инцидентами. 3. Игнорировать неопределённости. 4. Выбирать самую дорогую меру защиты «по умолчанию».

БЛОК Б (повышенный уровень) – Задание закрытого типа на установление соответствия
Инструкция: Прочитайте текст и установите соответствие

№ задания	Тексты заданий
11	Модель/политика ↔ Назначение: 1. Bell-LaPadula. 2. Biba. 3. RBAC. 4. Take-Grant. назначение: А. Контроль целостности Б. Контроль конфиденциальности. В. Роли и разрешения. Г. Передача прав.
12	Артефакт эксперимента ↔ Содержание 1. План эксперимента 2. Набор данных 3. Скрипт/проект 4. Отчёт Содержание А. Методика и метрики Б. Исходные значения и форматы В. Воспроизводимое выполнение Г. Результаты/выводы
13	Инструмент моделирования ↔ Применение: 1. Сеть Петри 2. IDEF0/IDEF3 3. Диаграмма потоков данных 4. Граф ролей; применение: А. Событийно-параллельные процессы Б. Функции/потоки управления В. Потоки данных между сущностями Г. Иерархия ролей и разрешений

№ задания	Тексты заданий
14	Метрика ↔ Интерпретация: 1. Кол-во нарушений/N шагов 2. Среднее время атаки 3. Доля доминируемых мер 4. Покрывание угроз характерное свойство А. Эффективность контроля доступа Б. Трудоёмкость достижения цели нарушителя В. Качество выбора по Парето. Г. Соответствие мер угрозам

БЛОК Б (повышенный уровень) – Задание закрытого типа на установление последовательности

Инструкция: Прочитайте текст и установите правильную последовательность

№ задания	Тексты заданий
15	Постановка и запуск эксперимента по МАС-политике: 1. Определить уровни/метки 2. Задать правила доступа 3. Сформировать сценарии доступа 4. Собрать метрики нарушений
16	Построение Парето-фронта для мер защиты: 1. Задать критерии (стоимость/эффект) 2. Оценить альтернативы 3. Исключить доминируемые 4. Выбрать компромиссы
17	Моделирование сети Петри для процесса атаки 1. Определить места/переходы 2. Задать начальные маркеры 3. Запустить симуляцию 4. Проанализировать достижимость/метрики

БЛОК В (высокий уровень) – Задание открытого типа с развернутым ответом

Инструкция: Прочитайте текст и запишите обоснованный ответ

№ задания	Тексты заданий
18	Инструкция: впишите недостающие термины/формулы в пропуски. F1. Заполните принцип модели Белла–ЛаПадуды: «нет _____ вверх и нет _____ вниз».
19	Инструкция: впишите недостающие термины/формулы в пропуски. F2. Запишите формулу ожидаемых потерь (risk exposure): _____ = _____ × _____ (обозначьте вероятность и ущерб).
20	Инструкция: впишите недостающие термины/формулы в пропуски. F3. Дополните определение сети Петри: «_____ хранят маркеры, а _____ срабатывают при выполнении условий, перевода маркеры».

Система оценивания выполнения тестовых заданий по компетенции ОПК-11

Номер задания	Указания по оцениванию	Результат оценивания (баллы, полученные за выполнение задания/характеристика правильности ответа)
Задания 1-10	Задания с выбором одного или нескольких верных ответов из предложенных считается верным, если правильно указана цифра или цифры, означающие верные ответы.	Совпадение с верным ответом оценивается 1 баллом; неверный ответ или его отсутствие - 0 баллов.
Задания 11-14	Задания закрытого типа на установление соответствия считается верным, если правильно установлены все соответствия (позиции из одного столбца верно сопоставлены с позициями другого)	Полное совпадение с верным ответом оценивается 1 баллом; неверный ответ или его отсутствие - 0 баллов.
Задания 15-17	Задания закрытого типа на установление последовательности считается верным, если правильно указана вся последовательность цифр	Полное совпадение с верным ответом оценивается 1 баллом; если допущены ошибки или ответ отсутствует- 0 баллов.
Задания 18-20	Задание открытого типа с развернутым ответом считается верным, если ответ совпадает с эталонным по содержанию и полноте.	Полный правильный ответ на задание оценивается 3 баллами; если допущена одна ошибка/неточность/ответ правильный, но не полный - 1 балл, если допущено более одной ошибки/ответ неправильный/ ответ отсутствует- 0 баллов.

Ключи к тестовым заданиям по оценке компетенции ОПК-11

№ задания	Верный ответ				
1	2				
2	1,2				
3	3				
4	2				
5	1,2				
6	1,2				
7	1				
8	1,2				
9	2				
10	1,2				
11	1	2	3	4	
	Б	А	В	Г	
12	1	2	3	4	
	А	Б	В	Г	
13	1	2	3	4	
	А	Б	В	Г	
14	1	2	3	4	
	А	Б	В	Г	
15	1, 2, 3, 4.				

16	1, 2, 3, 4.
17	1, 2, 3, 4.
18	чтения; записи
19	Ожидаемые потери = вероятность × ущерб
20	Места; переходы

Методические рекомендации по освоению дисциплины

1. Методические рекомендации преподавателю

Перед началом изучения дисциплины преподаватель должен ознакомить обучающихся с рабочей программой и оценочными материалами по дисциплине, с видами учебной и самостоятельной работы, перечнем литературы и интернет-ресурсов, с формами текущей и промежуточной аттестации, с критериями оценки качества знаний для итоговой оценки по дисциплине.

При проведении лекций, преподаватель:

- 1) формулирует тему и цель занятия, объявляет учебные вопросы;
- 2) излагает основные теоретические положения;
- 3) с помощью технических средств обучения и/или под запись дает определения основных понятий, расчетных формул;
- 4) проводит примеры из отечественного и зарубежного опыта, дает текущие статистические данные для наглядного и образного представления изучаемого материала;
- 5) в конце занятия выдает вопросы для самостоятельного изучения.

На занятиях лабораторного цикла следует обратить внимание на соответствие выбираемых обучающимся средств выполнения решаемым в работе задачам.

Каждая лабораторная работа должна быть оформлена и защищена в соответствии с требованиями. Защита производится после оформления отчета по работе.

Во время выполнения заданий в учебной аудитории обучающийся может консультироваться с преподавателем, определять наиболее эффективные методы решения поставленных задач. Если какая-то часть задания остается не выполненной, обучающийся может продолжить её выполнение во время внеаудиторной самостоятельной работы.

Для оценки полученных знаний и освоения учебного материала по каждому разделу и в целом по дисциплине преподаватель использует формы текущего, промежуточного и итогового контроля знаний обучающихся.

2. Методические рекомендации обучающимся

Приступая к изучению новой учебной дисциплины, обучающиеся должны ознакомиться с рабочей программой, оценочными материалами, учебной, научной и методической литературой, имеющейся в ЭИОС СКФ МТУСИ,

Глубина усвоения дисциплины зависит от активной и систематической работы обучающегося на лекциях и практических занятиях, а также в ходе самостоятельной работы, по изучению рекомендованной литературы.

2.1 Методические указания для обучающихся по лекционным занятиям

Важно сосредоточить внимание на содержании лекции. Это поможет лучше воспринимать учебный материал и уяснить взаимосвязь проблем по всей дисциплине.

Основное содержание лекции целесообразнее записывать в тетради в виде ключевых фраз, понятий, тезисов, обобщений, схем, опорных выводов. Необходимо обращать внимание на термины, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации. Желательно оставлять в конспектах поля, на которых делать пометки из рекомендованной литературы, дополняющей материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

С целью уяснения теоретических положений, разрешения спорных ситуаций необходимо задавать преподавателю уточняющие вопросы. Для закрепления содержания лекции в памяти, необходимо во время самостоятельной работы внимательно прочесть свой конспект и дополнить его записями из учебников и рекомендованной литературы.

Конспектирование читаемых лекций и их последующая доработка способствует более глубокому усвоению знаний, и поэтому являются важной формой учебной деятельности обучающихся.

2.2 Методические указания для обучающихся по подготовке к лабораторным работам

Лабораторные занятия по любой учебной дисциплине проводятся в соответствии с рабочей программой этой учебной дисциплины в установленные расписанием часы.

Инструктаж по технике безопасности, правилам пожарной безопасности и правилам внутреннего распорядка в лаборатории проводится преподавателем на первом лабораторном занятии. На этом же занятии обучающимся сообщаются:

- программа всего предстоящего лабораторного цикла;
- условия взаимодействия обучающихся с преподавателем в процессе выполнения лабораторных работ;
- условия контроля самостоятельной работы обучающихся, включая правила оформления отчетов по лабораторным работам и их последующей защиты;
- другая необходимая информация.

Организация лабораторных работ включает:

- самостоятельную внеаудиторную подготовку обучающегося к выполнению каждой отдельной лабораторной работы в соответствии с ее программой в рамках часов, выделенных на самостоятельную проработку материала в программе дисциплины;
- входной контроль преподавателем степени подготовленности каждого обучающегося к выполнению лабораторных работ;
- выполнение программы лабораторных работ в полном объеме;
- оформление отчета и его защиту каждым обучающимся в установленные сроки;
- формирование преподавателем рейтингов каждого из обучающихся по результатам выполнения и защиты им отдельных лабораторных работ и их циклов (используется Модульно-рейтинговая система).

Оценка качества выполнения лабораторных работ каждым обучающимся производится преподавателем отдельно за подготовку к работе, ее выполнение и защиту.

2.3 Методические указания для обучающихся по подготовке к практическим занятиям

Целью практических занятий является закрепление теоретических знаний, полученных при изучении дисциплины.

При подготовке к практическому занятию целесообразно выполнить следующие рекомендации:

- изучить основную литературу; ознакомиться с дополнительной литературой, новыми публикациями в периодических изданиях: журналах, газетах и т.д.;
- при необходимости доработать конспект лекций. При этом учесть рекомендации преподавателя и требования учебной программы.

При выполнении практических занятий основным методом обучения является самостоятельная работа обучающегося под управлением преподавателя. На них пополняются теоретические знания обучающихся, их умение творчески мыслить, анализировать, обобщать изученный материал, проверяется отношение обучающихся к будущей профессиональной деятельности.

Оценка выполненной работы осуществляется преподавателем комплексно: по результатам выполнения заданий, устному сообщению и оформлению работы.

После подведения итогов занятия обучающийся обязан устранить недостатки, отмеченные преподавателем при оценке его работы.

Для подготовки и выполнения практических занятий и лабораторных работ используются:

Бабаш, А. В. Моделирование системы защиты информации. Практикум: учебное пособие / Е.К. Баранова, А.В. Бабаш. — 3-е изд., перераб. и доп. — Москва: РИОР: ИНФРА-М, 2021. — 320 с. + Доп. материалы [Электронный ресурс]. — (Высшее образование). — DOI: <https://doi.org/10.29039/01848-4>. - ISBN 978-5-369-01848-4. - Текст : электронный. - URL: <https://znanium.com/catalog/product/>.

3. Методические рекомендации для обучающихся по самостоятельной работе

Самостоятельная работа обучающихся является составной частью учебной работы и имеет целью закрепление и углубление полученных знаний и навыков, поиск и приобретение новых знаний, в том числе с использованием автоматизированных обучающих курсов (систем), а также выполнение учебных заданий, подготовку к предстоящим занятиям, зачетам и экзаменам.

Самостоятельная работа во внеаудиторное время включает в себя:

- повторение лекционного материала;
- подготовки к лабораторным работам (практическим занятиям);
- изучения учебной и научной литературы;
- решения задач, выданных на практических занятиях;
- подготовки к тестированию;
- выделение наиболее сложных и проблемных вопросов по изучаемой теме, получение разъяснений и рекомендаций по данным вопросам с преподавателями кафедры на их еженедельных консультациях.

- проведение самоконтроля путем ответов на вопросы текущего контроля знаний, решения представленных в учебно-методических материалах кафедры задач, тестов, написания рефератов по отдельным вопросам изучаемой дисциплины.

Самостоятельная работа организуется преподавателями, обеспечивается и контролируется кафедрами. Она предусматривает, как правило, разработку рефератов, выполнение расчетно-графических, вычислительных работ, моделирования и других творческих заданий в соответствии с учебной программой (тематическим планом изучения дисциплины). Основная цель данного вида занятий состоит в обучении курсантов методам самостоятельной работы с учебным материалом.

Материал, подлежащий обработке на самостоятельных занятиях, намечается при разработке программы самостоятельной работы. Опыт, накопленный кафедрами в организации самостоятельных занятий, что материал выделяемый на такие занятия, должен удовлетворять следующим требованиям:

- быть изложенным в учебнике достаточно полно и с примерами;
- обеспечиваться достаточным количеством литературы, учебных пособий. учебно-методических материалов, образцов техники
- содержать материал. углубляющий знания, полученные на лекции;
- осваивать проблемные еще не полностью решенные вопросы.

Перед выполнением внеаудиторной самостоятельной работы преподаватель проводит инструктаж (консультацию) с определением цели задания, его содержания, сроков выполнения, основных требований к результатам работы, критериев оценки, форм контроля и перечня источников и литературы.

Обычно постановку задачи обучаемым на проведение самостоятельной работы преподаватель осуществляет на одном из занятий, предшествующему данному.

Методику самостоятельной работы все обучаемые выбирают индивидуально, но методика достижения конечной цели может определяться преподавателем и включать: последовательность изучения и усвоения учебно-методического материала, пособий, руководств, наставлений,

техники и т.д.; определение главного в изучаемом материале, материале, который необходимо законспектировать; просмотр учебных кинофильмов и их обсуждение; работу обучающихся по индивидуальным заданиям; опрос обучаемых в течении 7-10 минут с целью проверки усвоения главного из прочитанного материала.

При возникновении затруднений у обучаемых в разрешении вопросов задания преподавателю необходимо предусмотреть, чтобы каждый обучаемый мог получить оперативную консультацию по любому вопросу, если же при самостоятельной работе возникают затруднения по одному и тому же материалу (вопросу) у многих обучаемых, то желательно провести групповую консультацию.

Для контроля усвоения учебного материала целесообразно проводить в групповое собеседование или обсуждение изучаемого материала, проведение контрольных работ и т.п. Контрольные мероприятия при должной их организации позволяют не только оценивать знания материала, но и углубить и закрепить его у обучаемых.

Приветствуется использование компьютеров, которое:

- расширяет информационную базу учебных занятий;
- повышает активность обучаемых, из пассивного получателя информации они превращаются в её добытчиков:
- способствует развитию способностей к анализу и обобщению, улучшает связанность, широту и глубину мышления;
- облегчает усвоение абстрактного материала, позволяет многое из него представить в виде конкретных образов;
- приучает к точности, аккуратности, последовательности действий способствует развитию самостоятельности.

Компьютерные технологии и программные продукты для выполнения самостоятельной работы по освоению учебного материала необходимо использовать в соответствии с указаниями методических разработок раздела 5 настоящей Рабочей программы.

Для более углубленного изучения материала по дисциплине целесообразно использовать учебные курсы сайта <http://www.intuit.ru/>

Самостоятельная работа обучающихся над усвоением материала по дисциплине может выполняться в помещении для самостоятельной работы СКФ МТУСИ, посредством использования электронной библиотеки и ЭИОС.