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 УВР
_____А.Г. Жуковский
«29» 08 2022 г.

Моделирование систем защиты информации Б1.В.09
рабочая программа дисциплины

Кафедра: Инфокоммуникационные технологии и системы связи
Направление подготовки: **10.03.01 Информационная безопасность**
Профиль: **Безопасность компьютерных систем**
Формы обучения: **очная**

Распределение часов дисциплины по семестрам (для очной формы обучения), курсам (для заочной формы обучения)

Вид учебной работы	ОФ		ЗФ	
	ЗЕ	часов	ЗЕ	часов
Общая трудоемкость дисциплины, в том числе (по семестрам, курсам):	4	144/7сем		
Контактная работа, в том числе (по семестрам, курсам):		72/7сем		
Лекции		24/7сем		
Лабораторных работ		24/7сем		
Практических занятий		24/7сем		
Семинаров				
Самостоятельная работа		72/7сем		
Контроль				
Число контрольных работ (по курсам)				
Число КР (по семестрам, курсам)				
Число КП (по семестрам, курсам)				
Число зачетов с оценкой с разбивкой по семестрам (курсам)				
Число экзаменов с разбивкой по семестрам (курсам)		1/7сем		

Программу составил:
Доцент кафедры ИТСС к.т.н. Енгибарян И.А.

Рецензент:
Ведущий сотрудник ФГУП «РНИИРС», д.т.н., доцент Елисеев А.В.

Рабочая программа дисциплины
«Моделирование систем защиты информации»

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

Составлена на основании учебного плана
направления 10.03.01 «Информационная безопасность» профиля «Безопасность компьютерных систем», одобренного Учёным советом СКФ МТУСИ, протокол № 9 от 25.04.2022, и утвержденного директором СКФ МТУСИ 25.04.2022 г.

Рассмотрена и одобрена на заседании кафедры
«Инфокоммуникационные технологии и системы связи»

Протокол от «29» 08 2022 г. № 1

Зав. кафедрой _____ В.И. Юхнов

Визирование для использования в 20__/20__ уч. году

Утверждаю
Зам. директора по УВР ________________
«___» _______ 20__ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры

«Инфокоммуникационные технологии и системы связи»

Протокол от «___» _______ 20__ г. № ____
Зав. кафедрой _____________________

Визирование для использования в 20__/20__ уч. году

Утверждаю
Зам. директора по УВР ________________
«___» _______ 20__ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры

«Инфокоммуникационные технологии и системы связи»

Протокол от «___» _______ 20__ г. № ____
Зав. кафедрой _____________________

Визирование для использования в 20__/20__ уч. году

Утверждаю
Зам. директора по УВР ________________
«___» _______ 20__ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры

«Инфокоммуникационные технологии и системы связи»

Протокол от «___» _______ 20__ г. № ____
Зав. кафедрой _____________________

Визирование для использования в 20__/20__ уч. году

Утверждаю
Зам. директора по УВР ________________
«___» _______ 20__ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры

«Инфокоммуникационные технологии и системы связи»

Протокол от «___» _______ 20__ г. № ____
Зав. кафедрой _____________________

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 выпускника способности решать профессиональные задачи в соответствии с ***эксплуатационным*** видом деятельности:

Результатом освоения дисциплины являются сформированные у выпускника следующие компетенции:

Компетенции выпускника, формируемые 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.22 Информационные технологии и программирование
2	Б1.О.29 Основы управления информационной безопасностью
3	Б1.О.31 Безопасность компьютерных сетей
Последующие дисциплины и практики, для которых освоение данной дисциплины необходимо:	
1	Б1.О.39 Методы оценки безопасности компьютерных систем (Аудит компьютерных систем)
2	Б1.О.40 Администрирование средств защиты информации в комплексных системах и сетях

4. Структура и содержание дисциплины

4.1 Очная форма обучения, 4 года (всего 144 часа, 72 аудиторных часов, 72 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 (36+36) часов					
1.1	Основные понятия и определения, используемые при описании моделей безопасности компьютерных систем	Л 1	2	ОПК-11	Л1.1 Л1.2
1.2	Модели компьютерных систем с дискреционным управлением доступом	Л 2	2	ОПК-11	Л1.1 Л1.2
1.3	Пр №1. Модель решетки.	Пр 1	6	ОПК-11	Л 1.3
1.4	ЛР №1. Модель ХРУ и ТМД.	ЛР 1	6	ОПК-11	Л 1.3
1.5	Модели компьютерных систем с мандатным управлением доступом	Л 3	2	ОПК-11	Л1.1 Л1.2
1.6	Модели компьютерных систем с ролевым управлением доступом	Л 4	2	ОПК-11	Л1.1 Л1.2
1.7	Основные виды формальных моделей безопасности. Проблема адекватности реализации модели безопасности. Классическая модель Take-Grant. Расширенная модель Take-Grant.	СРС	18	ОПК-11	Л1.1 Л1.2
1.8	Модели безопасности информационных потоков	Л 5	2	ОПК-11	Л1.1 Л1.2
1.9	Модели безопасности управления доступом и информационными потоками	Л 6	2	ОПК-11	Л1.1 Л1.2
1.10	ЛР №2. Классическая модель Белла-ЛаПадулы и ее интерпретации	ЛР 2	6	ОПК-11	Л 1.3
1.11	ЛР №3 Модели ролевого управления доступом.	ЛР 3	6	ОПК-11	Л 1.3
1.12	ЛР №4 Модели безопасности информационных потоков.	ЛР 4	6	ОПК-11	Л 1.3
1.13	Дискреционные ДП-модели. Модель СВС. МРОСЛ ДП-модель.	СРС	12	ОПК-11	Л1.1 Л1.2 Л 1.3
Модуль 2. Методы моделирования систем защиты информации – 72 (36+36) часов					
2.1	Проектирование системы защиты информации с использованием модели с полным перекрытием множества угроз	Л 7	2	ОПК-11	Л1.1 Л1.2
2.2	Модель безопасности с полным перекрытием множества угроз	Пр.2	4	ОПК-11	Л2.1
2.3	Анализ рисков информационной безопасности	Л 8	2	ОПК-11	Л1.1 Л1.2
2.4	Анализ рисков информационной безопасности с использованием методики COBIT	Пр.3	6	ОПК-11	Л2.1
2.5	Система поддержки принятия Парето-оптимальных решений в области проектирования системы защиты информации	Л 9	2	ОПК-11	Л1.1 Л1.2

2.6	Метод принятия решений в разработке системы защиты информации на основе закона Парето и метода достижимых целей	Пр.4	4	ОПК-11	Л2.1
2.7	Анализ рисков информационной безопасности с использованием программного комплекса ГРИФ	СРС	4	ОПК-11	Л2.1
2.8	Моделирование на основе сети Петри	Л 10	2	ОПК-11	Л1.1 Л1.2
2.9	Разработка сценариев действий нарушителя ИБ с использованием сети Петри	Пр.5	4	ОПК-11	Л2.1
2.10	Методологии и стандарты IDEF для моделирования процессов в защищенных системах обработки информации	Л 11	2	ОПК-11	Л1.1 Л1.2
2.11	Использование методологии и стандарты IDEF для моделирования процессов в защищенных системах обработки информации	СРС	4	ОПК-11	Л2.1
2.12	Определение показателей защищенности информации при несанкционированном доступе. Методы расчета прочности оболочки защиты	СРС	6	ОПК-11	Л2.1
2.13	Анализ рисков ИБ для малого и среднего бизнеса. Матричный подход к анализу рисков информационной безопасности. Расчетная методика оценки рисков ИБ.	СРС	4	ОПК-11	Л2.1
2.14	Анализ и оценка рисков ИБ с использованием нечеткой логики. Построение оптимальной системы защиты информации.	Л 12	2	ОПК-11	Л1.1 Л1.2
	Экзамен подготовка		24		
	Итого		144		

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	Бабаш, А. В.	Моделирование системы защиты информации. Практикум : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 3-е изд., перераб. и доп. - URL: https://znanium.com/catalog/product/1232287	Москва : РИОР : ИНФРА-М, 2021. — 320 с.	Э1
Л.1.2	Богульская, Н. А.	Модели безопасности компьютерных систем : учебное пособие / Н. А. Богульская, М. М. Кучеров. - Красноярск : Сиб. федер. ун-т, 2019. - 206 с. - ISBN 978-5-7638-4008-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/1819309	Красноярск : Сиб. федер. ун-т, 2019. - 206 с. - ISBN 978-5-7638-4008-7	Э2
	Девянин, П. Н.	Модели безопасности компьютерных систем.Управление доступом и информац.потоками:Учебное пособие для вузов/П.Н.Девянин-2-е изд., испр. и доп.- ISBN 978-5-9912-0328-9, 100 экз. - Текст : электронный. - URL: https://znanium.com/catalog/product/436878	Москва :Гор.линия-Телеком,2013-338с.:ил.;. - (Специальность).	Э3

5.1.2. Дополнительная литература

Код	Авторы,	Заглавие	Издательство, год	Кол.

	составители			
Л2.1	Гришина, Н. В.	Основы моделирования процессов и систем защиты информации : учебное пособие / Н.В. Гришина. электронный. - URL: https://znanium.com/catalog/product/1891122.	Москва : ИНФРА-М, 2022. — 107 с.	Э4
Л2.2	Черняков, М. К.	Моделирование и проектирование производственных процессов и систем : учебное пособие / М. К. Черняков. - - URL: https://znanium.com/catalog/product/1866933.	Новосибирск : Изд-во НГТУ, 2020. - 94 с. - ISBN 978-5-7782-4249-4.	Э5

5.1.3. Учебно-методическое обеспечение для самостоятельной работы обучающихся

Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л3.1	Бабаш, А. В.	Моделирование системы защиты информации. Практикум : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 3-е изд., перераб. и доп. - URL: https://znanium.com/catalog/product/1232287	Москва : РИОР : ИНФРА-М, 2021. — 320 с.	Э1
Л3.2	Богульская, Н. А.	Модели безопасности компьютерных систем : учебное пособие / Н. А. Богульская, М. М. Кучеров. - Красноярск : Сиб. федер. ун-т, 2019. - 206 с. - ISBN 978-5-7638-4008-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/1819309	Красноярск : Сиб. федер. ун-т, 2019. - 206 с. - ISBN 978-5-7638-4008-7	Э2

5.2. Электронные образовательные ресурсы

Э1	https://znanium.com/catalog/product/1232287
Э2	https://znanium.com/catalog/product/1819309
Э3	https://znanium.com/catalog/product/436878
Э4	https://znanium.com/catalog/product/1891122.
Э5	https://znanium.com/catalog/product/1866933.

5.3. Программное обеспечение

П.1	Пакет Microsoft Office 2010
П.2	MS Word, MS Excel, Power Point - по лицензии
П.3	ПО «Coras»
П.4	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	Компьютерная аудитория с выходом в интернет
6.3 МТО рубежных контролей, экзамена	
1	Компьютерная аудитория

7. Методические указания для обучающихся по освоению дисциплины

7.1 Указания по самостоятельной работе студента

Достижение целей эффективной подготовки студентов в вузах невозможно без их целеустремленной самостоятельной работы. При этом, безусловно, нельзя обойтись без живого общения и консультирования со стороны профессорско-преподавательского состава Самостоятельная работа студентов 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. Обязательным компонентом самостоятельной работы студентов является внеаудиторный практикум по иностранному языку.

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.

Проведению самостоятельной работы (как и любого другого вида занятий) должна предшествовать подготовка как преподавателя, так и обучаемых.

Постановку задачи обучаемым на проведение самостоятельного занятия преподаватель осуществляет на одном из занятия, предшествующему данному. Он разъясняет смысл занятия и указывает, что к нему студенты должны приготовить. Задание на самостоятельную работу должно быть выдано заблаговременно с тем, чтобы слушатели имели время на информационный поиск в библиотеке необходимых пособий.

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 студентов 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 баз) 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/ .

Дополнения и изменения в рабочей программе