МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»
(РУТ (МИИТ)

Рабочая программа дисциплины (модуля),
как компонент образовательной программы
высшего образования - программы магистратуры
по направлению подготовки
10.04.01 Информационная безопасность,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Математические модели безопасности компьютерных систем и сетей

Направление подготовки: 10.04.01 Информационная безопасность

Направленность (профиль): Безопасность компьютерных систем и сетей

Форма обучения: Очная

1. Общие сведения о дисциплине (модуле).

Целью освоения учебной дисциплины «Математические модели безопасности компьютерных систем и сетей» является формирование компетенций по основным разделам дисциплины для целостного представления принципов использования математических моделей безопасности компьютерных систем (КС) и сетей.

Задачами дисциплины является формирование следующих навыков:

- применения математических моделей для разработки систем защиты компьютерных систем и сетей;
- анализа и проведения обоснованного выбор моделей и методов безопасности компьютерных систем и сетей;
- проводения эксперементалльных исследований защищенности объектов с учетом математических моделей безопасности компьютерных систем и сетей.

2. Планируемые результаты обучения по дисциплине (модулю).

Перечень формируемых результатов освоения образовательной программы (компетенций) в результате обучения по дисциплине (модулю):

ОПК-5 - Способен проводить научные исследования, включая экспериментальные, обрабатывать результаты исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи;

ПК-4 - Способность проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента.

Обучение по дисциплине (модулю) предполагает, что по его результатам обучающийся будет:

Знать:

-математические модели безопасности компьютерных систем и сетей, их применение при проведения экспериментальных исследований.

Уметь:

- разрабатывать модели
-угроз и модели нарушителя безопасности компьютерных систем и сетей;
-разрабатывать частные политики безопасности компьютерных системи

сетей, в том числе политики управления доступом и информационными потоками; применять методы моделирования безопасности КС и сетей;

-органзовывать научно-исследовательские работы в облати моделирования безопсности компьютерных систем и сетей, контролировать их выполнение и осущетвлять техническое и методичекое руководство.

Владеть:

-достаточными знаниями в теории математического моделировани, теории защиты информации и защиты компьютеных систем и сетей для проводения экспериментальных исследований защищенности объектов с применением соответствующих моделей, методов и средств обработки результатов эксперимента.

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 5 з.е. (180 академических часа(ов).

3.2. Объем дисциплины (модуля) в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Тип учебных занятий	Количество часов	
	Всего	Сем. №1
Контактная работа при проведении учебных занятий (всего):	48	48
В том числе:		
Занятия лекционного типа	16	16
Занятия семинарского типа	32	32

3.3. Объем дисциплины (модуля) в форме самостоятельной работы обучающихся, а также в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении промежуточной аттестации составляет 132 академических часа (ов).

3.4. При обучении по индивидуальному учебному плану, в том числе при ускоренном обучении, объем дисциплины (модуля) может быть реализован

полностью в форме самостоятельной работы обучающихся, а также в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении промежуточной аттестации.

4. Содержание дисциплины (модуля).

4.1. Занятия лекционного типа.

№ п/п	Тематика лекционных занятий / краткое содержание
1	1. ОСНОВНЫЕ ЭЛЕМЕНТЫ ТЕОРИИ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ Рассматриваемые вопросы: - понятия сущности, субъекта, доступа, права доступа, информационных потоков по памяти/по времени); - принципы и задачи создания защищенной компьютерной системы; - модели ценности информации: аддитивная модель, порядковая шкала, решетка многоуровневой безопасности. 2. УГРОЗЫ БЕЗОПАСНОСТИ, ПОЛИТИКА И МОДЕЛИ БЕЗОПАСНОСТИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ И СЕТЯХ Рассматриваемые вопросы: - понятие и классификация угроз безопасности информации, методы оценки угроз, модель нарушителя; - математические модели распространения компьютерных вирусов в сетях - RCS, двухфакторная модель, PSIDR, AAWP, на основе расчета длины гамильтонова пути; модели учитывающие структуру сети - случайный граф, двумерная решетка и иерархический случайный граф, и др.; - понятие политики безопасности, основные виды политик управления доступом и информационными потоками (политики дискреционного, мандатного, ролевого управления доступом, изолированной программной среды и безопасности информационных потоков). 3. МОДЕЛИ БЕЗОПАСНОСТИ НА ОСНОВЕ ДИСКРЕЦИОННОЙ, МАНДАТНОЙ, ТЕМАТИЧЕСКОЙ И РОЛЕВОЙ ПОЛИТИКИ Рассматриваемые вопросы: - общая характеристика моделей на основе дискреционной политики: модели на основе матрицы доступа, распространения прав доступа, HRU-модель, модель типизованной матрицы доступа, TAKE-GRANT; - модели на основе мандатной политики: модель Белла-ЛаПадулы и ее расширения; - модели на основе тематической политики: тематические решетки, модель тематико-иерархического разграничения доступа. 4. АВТОМАТНЫЕ И ТЕОРЕТИКО-ВЕРОЯТНОСТНЫЕ МОДЕЛИ НЕВЛИЯНИЯ И НЕВЫВОДИМОСТИ Рассматриваемые вопросы: - общая характеристика скрытых каналов утечки информации; - модели информационного невмешательства и информационной невыводимости; - нейтрализация скрытых каналов утечки информации на основе технологий "представлений" и "разрешенных процедур".

№ п/п	Тематика лекционных занятий / краткое содержание
	5. МЕТОДЫ И МОДЕЛИ ОБЕСПЕЧЕНИЯ ЦЕЛОСТНОСТИ И ДОСТУПНОСТИ (СОХРАННОСТИ) ДАННЫХ Рассматриваемые вопросы: - модели обеспечения целостности: общая характеристика моделей и технологий обеспечения целостности данных, дискреционная модель Кларка-Вильсона, мандатная модель Кена Биба; - доступность данных: резервирование, архивирование, журнализация данных; технологии репликации данных. 6. ПОЛИТИКА И МОДЕЛИ БЕЗОПАСНОСТИ В РАСПРЕДЕЛЕННЫХ КОМПЬЮТЕРНЫХ СИСТЕМАХ Рассматриваемые вопросы: - общая характеристика проблем безопасности в распределенных компьютерных системах; - модели распределенных систем в процессах разграничения доступа; - зональная модель разграничения доступа к информации в распределенных компьютерных системах. 7. ТЕОРЕТИКО-ГРАФОВЫЕ МОДЕЛИ КОМПЛЕКСНОЙ ОЦЕНКИ ЗАЩИЩЕННОСТИ Рассматриваемые вопросы: - "Комплексные оценки защищенности", агрегированная оценка; - система защиты в представленная х-дольным графом, примеры вариантов; - критерии технико-экономической эффективности. 8. МЕТОДЫ АНАЛИЗА И ОПТИМИЗАЦИИ ИНДИВИДУАЛЬНО-ГРУППОВЫХ СИСТЕМ РАЗГРАНИЧЕНИЯ ДОСТУПА Рассматриваемые вопросы: - теоретико-графовая модель системы индивидуально-групповых назначений доступа к иерархически организованным объектам; - пространственно-векторная модель; - характеристики системы рабочих групп пользователей.

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	1 ИССЛЕДОВАНИЕ ОБЩИХ ПРИНЦИПОВ СОЗДАНИЯ И ЭКСПЛУАТАЦИИ ЗАЩИЩЕННЫХ КОМПЬЮТЕРНЫХ СИСТЕМ. Результат работы – сравнительный анализ и описание принципов создания и эксплуатации ЗК систем. 2 КЛАССИФИКАЦИЯ УГРОЗ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ. Результат работы – пример классификации угроз КБ. 3 ИССЛЕДОВАНИЕ МОДЕЛИ HRU. Результат работы – построенный сценарий атаки. 4 ИССЛЕДОВАНИЕ МОДЕЛИ TAKE-GRAN. Результат работы – система команд перехода передачи субъекту прав доступа на объект от другого субъекта. 5 ИССЛЕДОВАНИЕ РАСШИРЕННОЙ МОДЕЛИ TAKE-GRAN. Результат работы – возможные неявные каналы чтения субъектом x информации из субъекта y, и

№ п/п	Тематика практических занятий/краткое содержание
	сравнение их стоимости. 6 ИССЛЕДОВАНИЕ МОДЕЛИ БЕЛЛА-ЛАПАДУЛЛЫ. Результат работы – система уровней допусков пользователей, грифов секретности объектов доступа, матрица доступа. 7 МОДЕЛЬ ТЕМАТИЧЕСКОГО РАЗГРАНИЧЕНИЯ ДОСТУПА НА ОСНОВЕ ИЕРАРХИЧЕСКИХ РУБРИКАТОРОВ. Результат работы – описание отношений доминирования, объединение и пересечение мультирубрик. 8 МОДЕЛЬ РОЛЕВОГО ДОСТУПА ПРИ ИЕРАРХИЧЕСКИ ОРГАНИЗОВАННОЙ СИСТЕМЕ РОЛЕЙ. Результат работы – описание ролей и полномочий. 9 АВТОМАТНАЯ МОДЕЛЬ ИНФОРМАЦИОННОГО НЕВЛИЯНИЯ GM-МОДЕЛЬ. Результат работы – описание GM-модели. 10 ХАРАКТЕРИСТИКИ МОДЕЛЕЙ ОБЕСПЕЧЕНИЯ ЦЕЛОСТНОСТИ ДАННЫХ. Результат работы – описание практического использования модели Кларка-Вильсона и мандатной модели Кена Биба для создания защищенных КС. 11 ЗОНАЛЬНАЯ МОДЕЛЬ РАЗГРАНИЧЕНИЯ ДОСТУПА. Результат работы – разработанная зональная структура КС, описание организации процессов пользователей к объектам КС, отображение множества пользователей на множество зон. 12 УПРАВЛЕНИЕ ДОСТУПОМ. Результат работы – правильная настройка системы. 13 ИССЛЕДОВАНИЕ МОДЕЛИ ТАМ. Результат работы – построенный граф отношений наследственности. 14 АНАЛИЗ ТЕХНИКО-ЭКОНОМИЧЕСКОЙ ЭФФЕКТИВНОСТИ СИСТЕМ ЗАЩИТЫ. Результат работы – расчет технико-экономической эффективности системы защиты. 15 АНАЛИЗ ТАКТИКО-ТЕХНИЧЕСКОЙ ЭФФЕКТИВНОСТИ СИСТЕМ ЗАЩИТЫ. Результат работы – расчет тактико-технической эффективности системы защиты. 16 МОДЕЛЬ АНАЛИЗА ИНДИВИДУАЛЬНО-ГРУППОВЫХ СИСТЕМ НАЗНАЧЕНИЯ ДОСТУПА К ИЕРАРХИЧЕСКИ ОРГАНИЗОВАННЫМ ОБЪЕКТАМ ДОСТУПА. Результат работы – составленная матрица смежности объектов доступа, матрица итоговой достижимости, итоговые права доступа.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Работа с лекционным материалом.
2	Подготовка к практическим занятиям.
3	Изучение дополнительной литературы.

4	Выполнение курсовой работы.
5	Подготовка к промежуточной аттестации.
6	Подготовка к текущему контролю.

4.4. Примерный перечень тем курсовых работ

Локальная оптическая сеть на три офисных здания.

Сеть на два офисных здания и отдельный центр обработки данных (проводная).

Локальная беспроводная сеть, объединяющая центральный офис, два филиала и ЦОД.

Локальная сеть, объединяющая центральный офис и 2 филиала.

Локальная беспроводная сеть, объединяющая центральный офис, филиал и 5 удаленных рабочих мест.

Локальная сеть с «чистой» ДМЗ.

Компьютерная система, состоящая из 2- небольших кластеров.

Беспроводная локальная сеть на 2 офисных здания.

Локальная оптическая сеть на 5 офисных зданий.

Локальная беспроводная сеть, объединяющая центральный офис и 5 удаленных рабочих мест.

Локальная беспроводная сеть, объединяющая центральный офис, филиал и 8 удаленных рабочих мест.

Беспроводная локальная сеть, объединяющая центральный офис и 3 филиала.

Беспроводная локальная сеть на 3 офисных здания.

Локальная сеть на три офисных здания и два отдельных центра обработки данных (проводная).

Два объединенных центра обработки данных.

Сеть CWDM с кольцевой физической топологией.

Локальная производственная сеть, включающая в свой состав несколько роботов.

Проводная локальная сеть, объединяющая центральный офис и 1 филиал и ЦОД.

Локальная проводная сеть, объединяющая центральный офис, 2 филиала и 3 удаленных рабочих места.

5. Перечень изданий, которые рекомендуется использовать при освоении дисциплины (модуля).

№ п/п	Библиографическое описание	Место доступа
1	Вострецова Е.В. Основы информационной безопасности: учебное пособие для студентов вузов. Екатеринбург: Изд-во Урал. ун-та, 2019.- 204 с. - ISBN 978-5-7996-2677-8.	https://elar.urfu.ru/bitstream/10995/73899/3/978-5-7996-2677-8_2019.pdf.(дата обращения: 29.01.2022). - Текст: электронный.
2	Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва: Издательство Юрайт, 2022. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2.	Образовательная платформа Юрайт [сайт].URL: https://urait.ru/bcode/497433 (дата обращения: 10.10.2022). - Текст: электронный
3	Голиков, А. М. Защита информации в инфокоммуникационных системах и сетях: учебное пособие / А. М. Голиков. — Москва: ТУСУР, 2015. — 284 с. // Лань: электронно-библиотечная система.	https://e.lanbook.com/book/110336(дата обращения: 04.10.2022).Режим доступа: для авториз.пользователей.Текст: электронный
4	Нестеров, С. А. Основы информационной безопасности: учебное пособие / С. А. Нестеров. — 5-е изд., стер. — Санкт-Петербург: Лань, 2022. — 324 с. — ISBN 978-5-8114-4067-2. Текст:	Лань: электронно-библиотечная система.https://e.lanbook.com/book/206279 (дата обращения: 04.10.2022).Режим доступа: для авториз. пользователей

	электронный	
5	Девянин П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. М.: Горячая линия – Телеком. 2020. – 352с. - ISBN 978-5-9912-0866-6.	Сайт издательства «Горячая линия - Телеком»http://www.techbook.ru/book.php?id_book=1137(дата обращения: 10.10.2022). -Текст непосредственный.
6	Буренин П.В., Девянин П.Н., Лебеденко Е.В. Безопасность операционной системы специального назначения Astra Linux Special Edition. версия 1.6 : учебное пособие / П. В. Буренин, П. Н. Девянин, Е. В. Лебеденко [и др.] ; под ред. П. Н. Девянина. - 2-е изд., перераб. и доп. - М.: Горячая линия - Телеком, 2021. - 404 с.: ил. - Библиогр.: с. 390-398. - ISBN 978-5-9912-0807-9	Библиотека РУТhttp://library.miit.ru/catalog/(дата обращения: 10.10.2022).Текст: непосредственный.

6. Перечень современных профессиональных баз данных и информационных справочных систем, которые могут использоваться при освоении дисциплины (модуля).

Форум специалистов по информационным технологиям http://citforum.ru/

Интернет-университет информационных технологий http://www.intuit.ru/

Поисковые системы: Yandex, Google, Mail.

Официальный сайт РУТ (МИИТ) (https://www.miit.ru/).

Научно-техническая библиотека РУТ (МИИТ) (http:/library.miit.ru).

Образовательная платформа «Юрайт» (https://urait.ru/).

Общие информационные, справочные и поисковые системы «Консультант Плюс», «Гарант».

Электронно-библиотечная система издательства «Лань» (http://e.lanbook.com/).

Электронно-библиотечная система ibooks.ru (http://ibooks.ru/).

7. Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства, необходимого для освоения дисциплины (модуля).

Microsoft Internet Explorer (или другой браузер).

Операционная система Microsoft Windows.

Microsoft Office.

В случае проведении занятий с применением электронного обучения и дистанционных образовательных технологий необходимо наличие компьютерной техники, для организации коллективных и индивидуальных форм общения педагогических работников со студентами, посредством используемых средств коммуникации. Допускается замена оборудования его виртуальными аналогами.

8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю).

- Для проведения аудиторных занятий и самостоятельной работы требуются:

Рабочее место преподавателя с персональным компьютером, подключённым к сетям INTERNET

Специализированная лекционная аудитория с мультимедиа аппаратурой и интерактивной доской.

Компьютерный класс с кондиционером. Рабочие места студентов в компьютерном классе, подключённые к сетям INTERNET

- Для проведения практических занятий:

компьютерный класс; кондиционер; компьютеры с минимальными требованиями – Pentium 4, ОЗУ 4 ГБ, HDD 100 ГБ, USB 2.0.

В случае проведении занятии с применением электронного обучения и дистанционных образовательных технологии необходимо наличие компьютернои техники, для организации коллективных и индивидуальных форм общения педагогических работников со студентами, посредством используемых средств коммуникации. Допускается замена оборудования его виртуальными аналогами.

9. Форма промежуточной аттестации:

Курсовая работа в 1 семестре.

Экзамен в 1 семестре.

10. Оценочные материалы.

Оценочные материалы, применяемые при проведении промежуточной аттестации, разрабатываются в соответствии с локальным нормативным актом РУТ (МИИТ).

Авторы

Профессор, доцент, д.н. кафедры «Вычислительные системы, сети и информационная безопасность»	Сафонова Ирина Евгеньевна

Лист согласования

Заведующий кафедрой ВССиИБ	Б.В. Желенков
Председатель учебно-методической комиссии	Н.А. Клычева