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 специалитета
по специальности
10.05.01 Компьютерная безопасность,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Модели безопасности компьютерных систем

Специальность: 10.05.01 Компьютерная безопасность

Специализация: Информационная безопасность объектов информатизации на базе компьютерных систем

Форма обучения: Очная

1. Общие сведения о дисциплине (модуле).

Целью изучения дисциплины «Модели безопасности компьютерных систем» является обучение специалистов принципам формального моделирования и анализа безопасности компьютерных систем (КС), реализующих управление доступом и информационными потоками, а также содействие фундаментализации образования, формированию научного мировоззрения и развитию системного мышления. Дисциплина «Модели безопасности компьютерных систем» относится к числу дисциплин специализации базовой части профессионального цикла.

Задачами изучения дисциплины являются: изучение основ устройства и принципов функционирования, методологии проектирования и построения защищенных, критериев и методов оценки защищенности КС, средств и методов защиты от несанкционированного доступа (НСД) к информации. Основной целью изучения учебной дисциплины «Модели безопасности компьютерных систем» является формирование у обучающегося компетенций для следующих видов деятельности: - научно-исследовательской; - специализация № 8. Дисциплина предназначена для получения знаний для решения следующих профессиональных задач (в соответствии с типами задач профессиональной деятельности): сбор, обработка, анализ и систематизация научно-технической информации, отечественного и зарубежного опыта по проблемам компьютерной безопасности; участие в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах; изучение и обобщение опыта работы других учреждений, организаций и предприятий по способам использования методов и средств обеспечения информационной безопасности с целью повышения эффективности и совершенствования работ по защите информации на конкретном объекте; разработка математических моделей защищаемых процессов и средств защиты информации и систем, обеспечивающих информационную безопасность объектов; специализации № 8 "Информационная безопасность объектов информатизации на базе компьютерных систем": разработка проектных решений и анализ систем обеспечения информационной безопасности объектов информатизации на базе компьютерных систем в защищенном исполнении и процессов их проектирования, создания и модернизации, в том числе разработка модели угроз и формирование требования к обеспечению информационной безопасности.

2. Планируемые результаты обучения по дисциплине (модулю).

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

ОПК-3 - Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности;

ОПК-9 - Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации;

ПК-2 - Способен применять математические методы в области компьютерной безопасности;

ПК-5 - Способен участвовать в работах по проектированию и реализации комплексного подхода к обеспечению информационной безопасности объекта защиты;

ПК-13 - Способен строить математические модели для оценки безопасности компьютерных систем и анализировать компоненты системы безопасности с использованием современных математических методов;

ПК-24 - Способен разрабатывать модели угроз, формировать требования по защите информации в объектах информатизации на базе компьютерных систем, а также процессов их проектирования, создания и модернизации.

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

Знать:

- Основные разделы фундаментальной и прикладной математики, необходимые для решения профессиональных задач (математический анализ, линейная алгебра, теория вероятностей, математическая логика, теория алгоритмов).
- Современные методы и средства защиты информации от утечки по техническим каналам (побочные электромагнитные излучения и наводки, акустические каналы и др.).
- Методы математической статистики и теории вероятностей, применяемые для обнаружения аномалий и атак в компьютерных системах.
- Принципы комплексного подхода (сочетание правовых, организационных, технических и криптографических мер) к защите объектов информатизации.

- Классы современных математических методов, применимых для анализа компонентов безопасности (теория массового обслуживания, марковские процессы, нечеткая логика, нейросетевые методы).

- Нормативные и методические документы (ФСТЭК, ФСБ) по разработке моделей угроз и определению требований к защите информации.

Уметь:

- Выявлять математическую сущность задачи профессиональной деятельности и строить ее формальную постановку.

- Выбирать и адаптировать методы защиты (криптографические, программно-аппаратные, организационные) под текущее состояние и тенденции развития информационных систем.

- Использовать вероятностно-статистические методы для анализа защищенности компьютерных систем и выявления вторжений.

- Анализировать существующую инфраструктуру объекта и предлагать меры по интеграции в нее средств защиты.

- Строить аналитические или имитационные модели, отражающие процессы функционирования механизмов защиты компьютерных систем.

- Разрабатывать частные модели угроз безопасности информации для конкретных информационных систем (включая описание источников угроз, уязвимостей, способов реализации).

Владеть:

- Навыками применения математического аппарата для построения моделей процессов и систем защиты информации.

- Навыками настройки и администрирования средств защиты информации в современных ОС, СУБД и сетевом оборудовании.

- Навыками проведения вычислительных экспериментов для оценки характеристик безопасности (вероятность взлома, время до отказа защиты).

- Навыками подготовки проектной и рабочей документации на различные этапы создания СЗИ.

- Навыками работы со средами имитационного моделирования (например, GPSS, AnyLogic) для оценки характеристик безопасности.

- Навыками работы с банками данных угроз и уязвимостей (например, БДУ ФСТЭК, CVE).

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 4 з.е. (144 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	Семестр №6
Контактная работа при проведении учебных занятий (всего):	96	96
В том числе:		
Занятия лекционного типа	48	48
Занятия семинарского типа	48	48

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 48 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	Введение. Рассматриваемые вопросы: - Основные понятия и определения - Основные элементы теории компьютерной безопасности. - Модели ценности информации. - Угрозы безопасности информации. - Политика безопасности.

№ п/п	Тематика лекционных занятий / краткое содержание
2	Модели компьютерных систем с дискреционным управлением доступа Рассматриваемые вопросы: - Модели компьютерных систем с дискреционным управлением доступа
3	Модель матрицы доступов Харрисона-Руззо-Ульмана (ХРУ). Рассматриваемые вопросы: - Модель матрицы доступов Харрисона-Руззо-Ульмана (ХРУ).
4	Модель типизированной матрицы доступов (ТМД). Рассматриваемые вопросы: - Модель типизированной матрицы доступов (ТМД).
5	Модель Take-Grant. Рассматриваемые вопросы: - Классическая модель распространения прав доступа Take-Grant. - Расширенная модель Take-Grant.
6	Алгоритм построения замыкания графа доступов и информационных потоков. Рассматриваемые вопросы: - Алгоритм построения замыкания графа доступов и информационных потоков.
7	Модели компьютерных систем с мандатным управлением доступа Рассматриваемые вопросы: - Модели компьютерных систем с мандатным управлением доступа
8	Классическая модель Белла-Ла Падулы. Рассматриваемые вопросы: - Особенности классическаой модель Белла-Ла Падулы. - Модель мандатной политики целостности информации Биба. - Интерпретации модели Белла-Ла Падулы.
9	Модели безопасности информационных потоков и изолированной программной среды Рассматриваемые вопросы: - особенности модели безопасности информационных потоков и изолированной программной среды
10	Автоматная, программная и вероятностная модели безопасности информационных потоков. Рассматриваемые вопросы: - Автоматная, программная и вероятностная модели безопасности информационных потоков.
11	Базовая теорема ИПС. Рассматриваемые вопросы: - Субъективно-ориентированная модель изолированной программной среды (ИПС). - Базовая теорема ИПС.
12	Модель ролевого управления доступом. Рассматриваемые вопросы: - Модели компьютерных систем с ролевым управлением доступа - Базовая модель ролевого управления доступом.
13	Модель административного ролевого управления доступом. Рассматриваемые вопросы: - Модель административного ролевого управления доступом.
14	Модель изолированной программной среды. Рассматриваемые вопросы: - Субъектно-ориентированная модель изолированной программной среды. - Безопасность информационных потоков.

№ п/п	Тематика лекционных занятий / краткое содержание
15	Модели безопасности компьютерных систем Рассматриваемые вопросы: - Развитие формальных моделей безопасности компьютерных систем
16	Модели безопасности КС. Рассматриваемые вопросы: - Взаимосвязь положений классических формальных моделей безопасности КС. - Проблема адекватности реализации модели безопасности в реальной КС.
17	Модели безопасности логического управления доступом и информационными потоками Рассматриваемые вопросы: - Семейство моделей безопасности логического управления доступом и информационными потоками (ДП-моделей).

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	Решетка многоуровневой безопасности. В результате выполнения практического задания студент получает навык исследования решетки многоуровневой безопасности
2	Теорема о передачи прав доступа В результате выполнения практического задания студент отрабатывает умение по применению теорем о передачи прав доступа
3	Теоремы об условиях реализации информационного потока В результате выполнения практического задания студент отрабатывает умение по применению теоремы об условиях реализации информационного потока
4	Построение замыкания графа доступов В результате выполнения практического задания студент получает навык постраения замыкания графа доступов
5	Модель ХРУ В результате выполнения практического задания студент получает навык постраения модели ХРУ
6	Сведение модели ХРУ к модели ТМД и наоборот В результате выполнения практического задания студент получает навык сведению модели ХРУ к модели ТМД и наоборот
7	Безопасность переходов В результате выполнения практического задания студент рассматривает особенности безопасных переходов.
8	Потенциальная модификация сущности В результате выполнения практического задания студент рассматривает основные потенциальные модификации сущности
9	Модель мандатного ролевого управления доступом В результате выполнения практического задания студент получает навык построения модели мандатного ролевого управления доступом

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Изучение дополнительной литературы.
2	Подготовка к практическим занятиям.
3	Выполнение курсовой работы.
4	Подготовка к промежуточной аттестации.
5	Подготовка к текущему контролю.

4.4. Примерный перечень тем курсовых работ

1. Анализ классической модели Take-Grant
2. Исследование модели решетки многоуровневой безопасности
3. Классическая модель Белла-ЛаПадулы и ее интерпретации
4. Построение замыкания графа доступов
5. Модель мандатного ролевого управления доступом
6. Модель Харрисона-Руззо-Ульмана (HRU)
7. Сведение модели HRU к модели ТМД и обратно
8. Модель административного ролевого управления доступом (ARBAC)
9. Анализ безопасности информационных потоков в автоматной модели
10. Модель изолированной программной среды
11. Исследование потенциальной модификации сущностей в моделях доступа
12. Модель целостности Биба
13. Анализ теорем о передаче прав доступа
14. ДП-модели (логическое управление доступом)
15. Вероятностная модель безопасности компьютерной системы

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

№ п/п	Библиографическое описание	Место доступа
1	Модели безопасности компьютерных систем Богульская Н. А., Кучеров М. М. Учебное пособие Сибирский Федеральный Университет, - 206 с. - ISBN 978-5-7638-4008-7 , 2019	https://reader.lanbook.com/book/157578

2	Модели безопасности компьютерных систем. Управление доступом и информационными потоками Девянин П.Н. Учебное пособие Издательство "Горячая линия-Телеком", - 2-е изд., испр. и доп., - 338 с. - ISBN 978-5-9912-0328-9 , 2017	https://reader.lanbook.com/book/111049

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

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.

Work 9, среда разработки программного обеспечения HTML5 и PHP.

Комплекс программ для ПЭВМ, обеспечивающих возможность выполнения работ: в области построения программных и аппаратных средств защиты информации в телекоммуникационных сетях (iOS15 Cisco и выше); программные продукты Mac OS server, XSan.

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

Учебные аудитории для проведения учебных занятий, оснащенные компьютерной техникой и наборами демонстрационного оборудования.

9. Форма промежуточной аттестации:

Курсовая работа в 6 семестре.

Экзамен в 6 семестре.

10. Оценочные материалы.

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

Авторы:

профессор, профессор, д.н. кафедры «Управление и защита информации» В.М. Алексеев

Согласовано:

Заведующий кафедрой УиЗИ Л.А. Баранов

Председатель учебно-методической комиссии С.В. Володин