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 - программа 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

Рабочая программа дисциплины (модуля) в виде электронного документа выгружена из единой корпоративной информационной системы управления университетом и соответствует оригиналу

Простая электронная подпись, выданная РУТ (МИИТ)
ID подписи: 2053
Подписал: заведующий кафедрой Баранов Леонид Аврамович
Дата: 01.06.2022

1. Общие сведения о дисциплине (модуле).

Дисциплина «Модели безопасности компьютерных систем» реализует требования федерального государственного образовательного стандарта высшего профессионального образования по направлению подготовки 100501 «Компьютерная безопасность». 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 ПСК-8 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 видами 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:

Уметь:

Применяет систему фундаментальных знании? (математических, естественнонаучных и инженерных) для формулирования и решения проблем задач защиты информации.

Уметь:

Применяет методы математического моделирования для формализации содержательно отчетливо сформулированных проблем.

Владеть:

Владеет методами и средствами моделирования политик безопасности, политик управления доступом и информационными потоками в компьютерных системах, угроз безопасности информации.

Знать:

Знает типовые модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах, угроз безопасности информации.

Уметь:

Умеет адаптировать типовые и строить оригинальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации.

Уметь:

Проводит анализ и разрабатывает под руководством квалифицированного специалиста математические модели безопасности компьютерных систем.

Владеть:

Применяет специальные математические методы, включая криптографические, для анализа и разработки защищенных компьютерных систем.

Уметь:

Применяет решения на основе специальных математических методов для обеспечения защищенной передачи данных в современных компьютерных сетях.

Знать:

Знать основные формальные модели изолированной программной среды и безопасности информационных потоков

Уметь:

Уметь разрабатывать модели угроз и модели нарушителя безопасности компьютерных систем.

Уметь:

Принимает участие в формировании политики информационной безопасности, ее реализации и контроле выполнения.

Уметь:

Формирует, организует и поддерживает комплекс мер по обеспечению информационной безопасности.

Уметь:

Строит математические модели для оценки безопасности компьютерных систем.

Уметь:

Анализирует компоненты системы безопасности с использованием современных математических методов

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 3 з.е. (108 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):	84	84
В том числе:		
Занятия лекционного типа	34	34
Занятия семинарского типа	50	50

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 24 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. Основные понятия и определения Основные элементы теории компьютерной безопасности. Модели ценности информации. Угрозы безопасности информации. Политика безопасности.
2	Модели компьютерных систем с дискреционным управлением доступа Модель матрицы доступов Харрисона-Руззо-Ульмана (ХРУ). Модель типизированной матрицы доступов (ТМД). Классическая модель распространения прав доступа Take-Grant. Расширенная модель Take-Grant. Алгоритм построения замыкания графа доступов и информационных потоков.
3	Модели компьютерных систем с мандатным управлением доступа Классическая модель Белла-Ла Падулы. Модель мандатной политики целостности информации Биба. Интерпретации модели Белла-Ла Падулы.
4	Модели безопасности информационных потоков и изолированной программной среды Автоматная, программная и вероятностная модели безопасности информационных потоков. Субъективно-ориентированная модель изолированной программной среды (ИПС). Базовая теорема ИПС.
5	Модели компьютерных систем с ролевым управлением доступа Базовая модель ролевого управления доступом. Модель административного ролевого управления доступом. Субъектно-ориентированная модель изолированной программной среды. Безопасность информационных потоков
6	Развитие формальных моделей безопасности компьютерных систем Взаимосвязь положений классических формальных моделей безопасности КС. Проблема адекватности реализации модели безопасности в реальной КС. 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	ПЗ1 Решетка многоуровневой безопасности
2	ПЗ2 Применение теорем о передачи прав доступа
3	ПЗ3 Применение теоремы об условиях реализации информационного потока
4	ПЗ4 Построение замыкания графа доступов
5	ПЗ5 Модель ХРУ
6	ПЗ6 Сведение модели ХРУ к модели ТМД и наоборот
7	ПЗ7 ПК1 - текущ. контроль по разделам 1,2,3

№ п/п	Тематика практических занятий/краткое содержание
8	ПЗ8 Безопасность переходов
9	ПЗ9 Потенциальная модификация сущности
10	ПЗ10 Модель мандатного ролевого управления доступом
11	ПЗ11 ПК2 - текущ. контроль по разделам 4, 5, 6.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	СР1 Модели ценности информации 1. Подготовка к практическому занятию. 2. Повторение лекционного материала. 3. Изучение учебной литературы из приведенных источников: [2, с.11-52], [доп. 2, стр.4-17]. 4. Изучение ресурсов информационно-телекоммуникационной сети «ИНТЕРНЕТ», необходимых для освоения дисциплины. 5. Конспектирование изученного материала по темам: Модели ценности информации
2	СР2 Модели ХРУ и ТМД. 1. Подготовка к практическому занятию. 2. Повторение лекционного материала. 3. Изучение учебной литературы из приведенных источников: [1 с.7-298,], [доп 2, с. с.19-72] . 4. Изучение ресурсов информационно-телекоммуникационной сети «ИНТЕРНЕТ», необходимых для освоения дисциплины. 5. Конспектирование изученного материала по темам: Модели ХРУ и ТМД. Классич
3	СР3 Модели решетки многоуровневой безопасности 1. Подготовка к практическому занятию. 2. Повторение лекционного материала. 3. Подготовка к текущему контролю. 4. Изучение учебной литературы из приведенных источников:, [1 с.7-298], [2 доп. с.69-103] 5. Изучение ресурсов информационно-телекоммуникационной сети «ИНТЕРНЕТ», необходимых для освоения дисциплины. 6. Конспектирование изученного материала по темам: Модели решетки многоуровневой безопасности.
4	СР4 Классическая модель Белла-Ла Падулы 1. Подготовка к практическому занятию. 2. Повторение лекционного материала. 3. Изучение учебной литературы из приведенных источников: [1 с.7-298], [2 доп. с.157-170]. 4. Изучение ресурсов информационно-телекоммуникационной сети «ИНТЕРНЕТ», необходимых для освоения дисциплины. 5. Конспектирование изученного материала по темам: Классическая модель Белла-Ла Падулы
5	СР5 Модель ролевого управления доступом. Иерархия ролей в модели мандатного ролевого управления доступом. 1. Подготовка к практическому занятию. 2. Повторение лекционного материала. 3. Изучение учебной литературы из приведенных источников: [1 с.7-298], [2 доп. с.234-253]. 4. Изучение ресурсов информационно-телекоммуникационной сети «ИНТЕРНЕТ», необходимых для освоения дисциплины. 5. Конспектирование изученного материала по темам: Модель ролевого управления доступом. Иерархия ролей в модели мандатного ролевого управления доступом.
6	СР6 Анализ в рамках ДП-моделей информационных потоков по памяти или по времени

№ п/п	Вид самостоятельной работы
	1. Подготовка к практическому занятию. 2. Повторение лекционного материала. 3. Подготовка к текущему контролю. 4. Изучение учебной литературы из приведенных источников: [1 с.7-298], [2 доп. с. 199-230] 5. Изучение ресурсов информационно-телекоммуникационной сети «ИНТЕРНЕТ», необходимых для освоения дисциплины. 6. Конспектирование изученного материала по темам: Анализ в рамках ДП-моделей информационных потоков по памяти или по времени.
7	Выполнение курсовой работы.
8	Подготовка к промежуточной аттестации.
9	Подготовка к текущему контролю.

4.4. Примерный перечень тем курсовых работ

Курсовые работы (проекты) не предусмотрены

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

№ п/п	Библиографическое описание	Место доступа
1	Информационная безопасность и защита информации В.П. Мельников, С.А. Клейменов, А.М. Петраков Книга Издательский центр "Академия" , 2012	ИТБ УЛУПС (Абонемент ЮИ); ИТБ УЛУПС (ЧЗ1 ЮИ)
2	Модели безопасности компьютерных систем П.Н. Девянин Однотомное издание Академия , 2005	НТБ (фб.)
3	Информационная безопасность и защита информации в корпоративных сетях железнодорожного транспорта В.В. Яковлев, А.А. Корниенко Однотомное издание УМК МПС России , 2002	НТБ (уч.4); НТБ (фб.); НТБ (чз.1)
1	Модели безопасности компьютерных систем. Управление доступом и информационными потоками Девянин П.Н. М: Горячая линия-Телеком , 2011	НТБ (фб.)
2	Применение объектно-ориентированных моделей разграничения доступа к анализу безопасности ряда компьютерных систем (Математические структуры и моделирование №2, 2016). С.В. БЕЛИМ , С.В. УСОВ Лань, , 2016	ЭБС Лань; elibrary.ru

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

http://library.miit.ru/ - электронно-библиотечная система Научно-технической библиотеки МИИТ. http://elibrary.ru/ - научно-электронная библиотека. http://robotosha.ru/ www.chipinfo.ru. http://siblec.ru/ http://autex.ru/

http://www.intuit.ru http://twirpx.com http://habrahabr.ru http://semestr.ru htth://www.cisco.ru

Поисковые системы: Yandex, Google, Mail, база научно-технической информации ВИНИТИ РАН.

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

Для проведения лекционных занятий необходима

специализированная лекционная аудитория с мультимедиа аппаратурой и интерактивной доской.

Для проведения практических занятий

необходимы компьютеры с рабочими местами в компьютерном классе. Компьютеры должны быть обеспечены лицензионными программными продуктами: Microsoft Office или Work 9, среда разработки программного обеспечения HTML5 и PHP. Для проведения практических занятий и необходимо иметь 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).

Для проведения аудиторных занятий и самостоятельной работы требуется:1. Рабочее место преподавателя с персональным компьютером, подключённым к сетям INTERNET и INTRANET. 2. Специализированная лекционная аудитория с мультимедиа аппаратурой и интерактивной доской. 3. Компьютерный класс. Рабочие места студентов в компьютерном классе, подключённые к сетям INTERNET и INTRANETДля проведения практических занятий:компьютерный класс; компьютеры с минимальными требованиями – Core 5, ОЗУ 4 ГБ, HDD 300 ГБ, wifi, USB 2.0.

9. Форма промежуточной аттестации:

Зачет в 6 семестре.

Курсовая работа 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