МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА (МИИТ)»

УТВЕРЖДАЮ:

Директор ИТТСУ

П.Ф. Бестемьянов

08 сентября 2017 г.

Кафедра «Управление и защита информации»

Автор Алексеев Виктор Михайлович, д.т.н., профессор

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

«Модели безопасности компьютерных систем»

Специальность:	10.05.01 – Компьютерная безопасность
Специализация:	Информационная безопасность объектов информатизации на базе компьютерных систем
Квалификация выпускника:	Специалист по защите информации
Форма обучения:	очная
Год начала подготовки	2017

Одобрено на заседании	Одобрено на заседании кафедры
Учебно-методической комиссии института Протокол № 1 06 сентября 2017 г. Председатель учебно-методической комиссии  С.В. Володин	Протокол № 2 04 сентября 2017 г. Заведующий кафедрой  Л.А. Баранов

Москва

1. Цели освоения учебной дисциплины

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;
- проектной;
- контрольно-аналитической.
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;

проектная деятельность:
разработка и конфигурирование программно-аппаратных средств защиты информации;
разработка технических заданий на проектирование, эскизных, технических и рабочих проектов систем и подсистем защиты информации с учетом действующих нормативных и методических документов;
разработка проектов систем и подсистем управления информационной безопасностью объекта в соответствии с техническим заданием;
проектирование программных и аппаратных средств защиты информации в соответствии с техническим заданием с использованием средств автоматизации проектирования;

контрольно-аналитическая деятельность:
оценивание эффективности реализации систем защиты информации и действующей политики безопасности в компьютерных системах;
предварительная оценка, выбор и разработка необходимых методик поиска уязвимостей;
применение методов и методик оценивания безопасности компьютерных систем при

проведении контрольного анализа системы защиты;
выполнение экспериментально-исследовательских работ при проведении сертификации программно-аппаратных средств защиты и анализ результатов;
проведение экспериментально-исследовательских работ при аттестации объектов с учетом требований к обеспечению защищенности компьютерной системы;
проведение инструментального мониторинга защищенности компьютерных систем;
подготовка аналитического отчета по результатам проведенного анализа и выработка предложений по устранению выявленных уязвимостей.

2. Место учебной дисциплины в структуре ОП ВО

Учебная дисциплина "Модели безопасности компьютерных систем" относится к блоку 1 "Дисциплины (модули)" и входит в его базовую часть.

3. Планируемые результаты обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы

Процесс изучения дисциплины направлен на формирование следующих компетенций:

ПК-4	способностью проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем
ПСК-8.1	способностью разрабатывать модели угроз, формировать требования к обеспечению информационной безопасности объектов информатизации на базе компьютерных систем в защищенном исполнении и процессов их проектирования, создания и модернизации

4. Общая трудоемкость дисциплины составляет

4 зачетные единицы (144 ак. ч.).

5. Образовательные технологии

Преподавание дисциплины «Модели безопасности компьютерных систем» осуществляется в форме лекций, лабораторных работ и практических занятий.Лекции проводятся в традиционной классно-урочной организационной форме, по типу управления познавательной деятельностью на 30 % являются традиционными классически-лекционными (объяснительно-иллюстративные), и на 70 % с использованием интерактивных (диалоговых) технологий, в том числе мультимедиа лекция (18 часов).Практические занятия и лабораторные работы организованы с использованием технологий развивающего обучения. Часть практического курса выполняется в виде традиционных практических занятий (объяснительно-иллюстративное решение задач). Остальная часть практического курса проводится с использованием интерактивных (диалоговые) технологий, в том числе электронный практикум (решение проблемных поставленных задач с помощью современной вычислительной техники и исследование моделей); технологий, основанных на коллективных способах обучения, а так же использованием компьютерной тестирующей системы.В ходе выполнения курсовой работы реализуются проектные и исследовательские методы обучения. Это позволяет развивать индивидуальные творческие способности обучающихся, более осознанно подходить к профессиональному и социальному самоопределению, самостоятельно пополнять свои знания, глубоко вникать в изучаемую проблему и предполагать пути ее решения, что важно при формировании мировоззрения. Это важно для определения индивидуальной траектории развития каждого обучающегося.Самостоятельная работа студента организована с использованием традиционных видов работы и интерактивных технологий. К традиционным видам работы относятся отработка лекционного материала и

отработка отдельных тем по учебным пособиям. К интерактивным (диалоговым) технологиям относиться отработка отдельных тем по электронным пособиям, подготовка к промежуточным контролям в интерактивном режиме, интерактивные консультации в режиме реального времени по специальным разделам и технологиям, основанным на коллективных способах самостоятельной работы студентов.Оценка полученных знаний, умений и навыков основана на модульно-рейтинговой технологии. Весь курс разбит на 6 разделов, представляющих собой логически завершенный объём учебной информации. Фонды оценочных средств освоенных компетенций включают как вопросы теоретического характера для оценки знаний, так и задания практического содержания (решение конкретных задач, работа с данными) для оценки умений и навыков. Теоретические знания проверяются путём применения таких организационных форм, как индивидуальные и групповые опросы, решение тестов с использованием компьютеров или на бумажных носителях..

6. Содержание дисциплины (модуля), структурированное по темам (разделам)

РАЗДЕЛ 1
Введение. Основные понятия и определения
Основные элементы теории компьютерной безопасности.
Модели ценности информации.
Угрозы безопасности информации. Политика безопасности.

РАЗДЕЛ 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.

РАЗДЕЛ 3
Модели компьютерных систем с мандатным управлением доступа
Классическая модель Белла-Ла Падулы.
Модель мандатной политики целостности информации Биба. Интерпретации модели Белла-Ла Падулы.

РАЗДЕЛ 3
Модели компьютерных систем с мандатным управлением доступа
Устный опрос

РАЗДЕЛ 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.

РАЗДЕЛ 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.

РАЗДЕЛ 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).

РАЗДЕЛ 6
Развитие формальных моделей безопасности компьютерных систем
Устный опрос

РАЗДЕЛ 7
Зачет с оценкой