МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»

Кафедра «Вычислительные системы, сети и информационная безопасность»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

«Методы оценки безопасности компьютерных систем»

Направление подготовки:	10.03.01 – Информационная безопасность
Профиль:	Безопасность компьютерных систем
Квалификация выпускника:	Бакалавр
Форма обучения:	очная
Год начала подготовки	2020

1. Цели освоения учебной дисциплины

Целями освоения учебной дисциплины «Методы оценки безопасности компьютерных систем» являются формирование компетенций по основным разделам данного курса, изучение студентами основных методов оценки безопасности компьютерных систем, стандартов в этой области; получение представления об организации и принципах обеспечения информационной безопасности компьютерных систем.
Студенты должны научиться применять современные методы оценки безопасности компьютерных систем.

Дисциплина формирует знания и умения для решения следующих профессиональных задач (в соответствии с видами профессиональной деятельности):

Эксплуатационной:
- установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований;
- администрирование подсистем информационной безопасности объекта;
- участие в проведении аттестации объектов информатизации по требованиям безопасности информации и аудите информационной безопасности автоматизированных систем;

Проектно-технологической:
- сбор и анализ исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности;
- проведение проектных расчетов элементов систем обеспечения информационной безопасности;
- участие в разработке технологической и эксплуатационной документации;
проведение предварительного технико-экономического обоснования проектных расчетов;

Организационно-управленческой:
- осуществление организационно-правового обеспечения информационной безопасности объекта защиты;
- организация работы малых коллективов исполнителей;
- участие в совершенствовании системы управления информационной безопасностью;
- изучение и обобщение опыта работы других учреждений, организаций и предприятий в области защиты информации, в том числе информации ограниченного доступа;
- контроль эффективности реализации политики информационной безопасности объекта защиты.

Экспериментально-исследовательской:
- сбор, изучение научно-технической информации, отечественного и зарубежного опыта по тематике исследования;
- проведение экспериментов по заданной методике, обработка и анализ их результатов;
проведение вычислительных экспериментов с использованием стандартных программных средств.

2. Место учебной дисциплины в структуре ОП ВО

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

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

Процесс изучения дисциплины направлен на формирование следующих компетенций:

ПКР-2	Способность участвовать в разработке политик безопасности, политик управления доступом и информационными потоками в компьютерных сетях

4. Общая трудоемкость дисциплины составляет

3 зачетные единицы (108 ак. ч.).

5. Образовательные технологии

Преподавание дисциплины «Методы оценки безопасности компьютерных систем» осуществляется в форме лекций и практических занятий.Лекции проводятся в традиционной классно-урочной организационной форме в объеме 18 часов, по типу управления познавательной деятельностью на 100% являются традиционными классически-лекционными (объяснительно-иллюстративными). Практические работы (18 часов) организованы с использованием технологий развивающего обучения. Самостоятельная работа студента организована с использованием традиционных видов работы. К традиционным видам работы (72 часа) относится отработка лекционного материала.Весь курс разбит на 5 разделов, представляющих собой логически завершенный объем учебной информации. Фонды оценочных средств освоенных компетенций включают вопросы теоретического характера для оценки знаний. Теоретические знания проверяются путем применения таких организационных форм, как индивидуальные и групповые опросы. .

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

РАЗДЕЛ 1
Обеспечение информационной безопасности.
контрольная работа №1)

Тема: Формальные методы доказательства правильности программ и их спецификаций

Тема: Методы и средства анализа безопасности программного обеспечения (контрольно-испытательные методы логико-аналитические методы).

Тема: Федеральные критерии безопасности информационных технологий.

Тема: Защита АС и средств СВТ.

Тема: Стандарты безопасности в сети Internet.
(контрольная работа №1)

РАЗДЕЛ 2
Критерии оценки пригодности компьютерных систем TCSEC (Оранжевая книга).
Критерии безопасности компьютерных систем СТСРЕС.

Тема: TCSEC (Основные группы безопасности)
группа D, C, B, A. Классы безопасности
(класс C1 - Discretionary Security Protection, класс C2 - Controlled Access Protection, класс B1 - Labeled Security Protection, класс B3 - Security Domains; класс A1

Тема: TCPEC
критерии конфиденциальности - контроль скрытых каналов; произвольное управление доступом; нормативное управление доступом; повторное использование объектов; критерии целостности - домены целостности; произвольное управление целостностью; нормативное управление целостностью; физическая целостность; возможность осуществления отката; разделение ролей; самотестирование; критерии работоспособности -контроль за распределением ресурсов; устойчивость к отказам и сбоям; живучесть; восстановление; критерии аудита (регистрация и учет событий в системе; идентификация и аутентификация

РАЗДЕЛ 3
Гармонизированные критерии оценки безопасности информационных технологий ITSEC.

Тема: Гарантированность безопасности (семь возможных уровней гарантированности корректности - от E0 до E6; общая оценка системы).
(группа D - Minimal Protection (минимальная защита); группа C - Discretionary Protection (избирательная защита); группа B - Mandatory Protection (полномочная защита)
группа A - Verified Protection (проверяемая защита)).

Тема: Сетевые конфигурации (требования к обеспечению конфиденциальности и целостности информации в сетевых конфигурациях).
(класс C1 - Discretionary Security Protection (избирательная защита безопасности) ; класс C2 - Controlled Access Protection (защита контролируемого доступа),класс B1 - Labeled Security Protection (меточная защита безопасности); класс B3 - Security Domains (области безопасности); класс A1 - Verified Desing (проверяемая разработка))

РАЗДЕЛ 4
Рекомендации X.800 для распределенных систем
контрольная работа №2

Тема: Функции или сервисы безопасности (аутентификация; управление доступом; конфиденциальность данных; целостность данных; неотказуемость; реализация функций безопасности по уровням эталонной модели OSI).

Тема: . Механизмы безопасности (шифрование; ЭП; дополнения трафика; управление маршрутизацией; нотаризация).

Тема: Взаимосвязь функций и механизмов безопасности.

Тема: Администрирование средств безопасности (администрирование системой; сервисами безопасности; механизмами безопасности).

РАЗДЕЛ 5
Общие критерии оценки безопасности информационных технологий.

Тема: Классификация набора требований безопасности (общие положения, структуры группирования и принципы целевого использования требований безопасности).

Тема: Объект оценки (понятие, представление и общая модель).

Тема: Требования безопасности (требования к функциям безопасности, требования гарантии безопасности).

Тема: Критерии оценки для профилей защиты.

РАЗДЕЛ 7
Итоговая аттестация