

**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:	<u>10.03.01 – Информационная безопасность</u>
Профиль:	<u>Безопасность компьютерных систем</u>
Квалификация выпускника:	<u>Бакалавр</u>
Форма обучения:	<u>очная</u>
Год начала подготовки	<u>2017</u>

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.

Основными задачами дисциплины являются:

- Ознакомление с оценочными стандартами и техническими спецификациями.
- Изучение методов оценки безопасности компьютерных систем.
- Изучение формальных и неформальных средств защиты.
- Изучение стандартов информационной безопасности.

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

Эксплуатационная:

- 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-технологическая:

- 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

Экспериментально-исследовательская деятельность:

- 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

Организационно-управленческая деятельность:

- 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.

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 базовую часть.

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

Процесс изучения дисциплины направлен на формирование следующих компетенций:

ПСК-1.2	способность использовать математические методы обработки, анализа и синтеза результатов профессиональных исследований (ПСК 1.2);
---------	--

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 14 часов, по типу управления познавательной деятельностью на 100% являются традиционными классически-лекционными (объяснительно-иллюстративными). Практические работы (28 часов) организованы с использованием технологий развивающего обучения, проводится с использованием интерактивных (диалоговых) технологий, в том числе электронный практикум (решение проблемных поставленных задач с помощью современной вычислительной техники); технологий, основанных на коллективных способах обучения. Самостоятельная работа студента организована с использованием традиционных видов работы. К традиционным видам работы (66 часов) относится отработка лекционного материала. Оценка полученных знаний, умений и навыков основана на модульно-рейтинговой технологии. Весь курс разбит на 5 разделов, представляющих собой логически заверченный 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. Проведении занятий по дисциплине (модулю) возможно с применением электронного обучения и дистанционных образовательных технологий, реализуемые с применением информационно-телекоммуникационных сетей при опосредованном (на расстоянии) взаимодействии обучающихся и педагогических работников. В процессе проведения занятий с применением электронного обучения и дистанционных образовательных технологий применяются современные образовательные технологии, такие как (при необходимости): - использование современных средств коммуникации; - электронная форма обмена материалами; - дистанционная форма групповых и индивидуальных консультаций; - использование компьютерных технологий и программных продуктов, необходимых для сбора и систематизации информации, проведения требуемых программой расчетов и т.д..

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

РАЗДЕЛ 1

Обеспечение информационной безопасности.

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 безопасности компьютерных систем СТСПЕС. Рекомендации X.800 для распределенных систем.

Тема: Функциональные критерии. Критерии конфиденциальности (контроль скрытых каналов; произвольное управление доступом; нормативное управление доступом; повторное использование объектов).

Тема: Критерии целостности (домены целостности; произвольное управление целостностью; нормативное управление целостностью; физическая целостность; возможность осуществления отката; разделение ролей; самотестирование).

Тема: Критерии работоспособности (контроль за распределением ресурсов; устойчивость к отказам и сбоям; живучесть; восстановление).

Тема: Критерии аудита (регистрация и учет событий в системе; идентификация и аутентификация).

РАЗДЕЛ 3

Критерии оценки пригодности компьютерных систем TCSEC (Оранжевая книга).

Тема: Основные группы безопасности
(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: Классы безопасности
(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 Design (проверяемая разработка))

РАЗДЕЛ 4

Гармонизированные критерии оценки безопасности информационных технологий ITSEC.

Тема: Гарантированность безопасности (семь возможных уровней гарантированности корректности - от E0 до E6; общая оценка системы).

Тема: Требования к политике безопасности (требования к наличию защитных механизмов; дополнительные классы).

Тема: Сетевые конфигурации (требования к обеспечению конфиденциальности и целостности информации в сетевых конфигурациях).
(контрольная работа №2)

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