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

«Защита программ и данных»

Направление подготовки:	10.03.01 – Информационная безопасность
Профиль:	Безопасность компьютерных систем
Квалификация выпускника:	Бакалавр
Форма обучения:	очная
Год начала подготовки	2017

1. Цели освоения учебной дисциплины

Целью освоения учебной дисциплины «Защита программ и данных» является формирование компетенций в области в области защиты программ и данных от воспроизведения, исследования, модификации.
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 "Защита программ и данных" 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:

ОПК-7	способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты

ПК-3	способностью администрировать подсистемы информационной безопасности объекта защиты

4. Общая трудоемкость дисциплины составляет

3 зачетные единицы (108 ак. ч.).

5. Образовательные технологии

Преподавание дисциплины «Защита программ и данных» осуществляется в форме лекций и лабораторных занятий.Лекции (18 часов) проводятся в традиционной организационной форме с применением проекционного оборудования.Лабораторные занятия (26 часов) проводятся в компьютерном классе, подключенном к локальной сети кафедры. Необходим доступ в сеть МИИТа (требуется доступ к KMS серверу).Самостоятельная работа студента организована с использованием традиционных видов работы. К традиционным видам работы (64 часа) относится отработка лекционного материала и подготовка к лабораторным работам Оценка полученных знаний, умений и навыков основана на модульно-рейтинговой технологии. Весь курс разбит на 3 раздела, представляющих собой логически завершенный объем учебной информации. Фонды оценочных средств освоенных компетенций включают как вопросы теоретического характера для оценки знаний, так и описание лабораторных работ. 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
ЗАЩИТА ПРИ СОЗДАНИИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Тема: Недокументированные возможности. Закладки. Обфускация кода.

Тема: Методы, затрудняющие чтение исходного текста и декомпиляцию. Обфускация кода

Тема: Тестирование программного обеспечения.

Тема: Сокрытие присутствия программы в системе. Исполнение данных как кода. Повышение привилегий.

РАЗДЕЛ 2
ЗАЩИТА КОМПЬЮТЕРНЫХ СИСТЕМ ОТ ВРЕДОНОСНЫХ ПРОГРАММ

Тема: Классификация вредоносных программ. Основные информационные ресурсы по вредоносным программам.

Тема: Методы обнаружения известных вредоносных программ.

Тема: Методы обнаружения неизвестных вредоносных программ.

Тема: Настройка операционной системы, повышающая ее безопасность.

Тема: Сетевые средства борьбы с вредоносными программами.

Тема: Средства защиты от вредоносных программ. Сравнение основных средств защиты. Выполнение лабораторной работы № 1

РАЗДЕЛ 3
ЗАЩИТА КОМПЬЮТЕРНЫХ ПРОГРАММ ОТ НЕСАНКЦИОНИРОВАННОГО ИСПОЛЬЗОВАНИЯ

Тема: Основные способы защиты программного обеспечения от несанкционированного использования. Серийный номер. Привязка к аппаратной конфигурации компьютера. Online и Offline активация.

Тема: Аппаратные средства защиты от несанкционированного использования. USB ключ

Тема: Сетевые средства защиты от несанкционированного использования. FlexNET.

Дифференцированный зачет