МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА (МИИТ)»

УТВЕРЖДАЮ:

Директор РОАТ

В.И. Апатцев

29 мая 2018 г.

Кафедра «Железнодорожная автоматика, телемеханика и связь»

Автор Ермаков Александр Евгеньевич, к.т.н., доцент

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

«Системы обнаружения компьютерных атак»

Направление подготовки:	09.04.03 – Прикладная информатика
Магистерская программа:	Прикладная информатика в обеспечении безопасности бизнеса
Квалификация выпускника:	Магистр
Форма обучения:	заочная
Год начала подготовки	2018

Одобрено на заседании	Одобрено на заседании кафедры
Учебно-методической комиссии института Протокол № 2 22 мая 2018 г. Председатель учебно-методической комиссии С.Н. Климов	Протокол № 10 15 мая 2018 г. Заведующий кафедрой А.В. Горелик

Москва 2018 г.

1. Цели освоения учебной дисциплины

Целью освоения учебной дисциплины «Системы обнаружения компьютерных атак» является формирование у обучающихся компетенций в соответствии с федеральными государственными образовательными стандартами по специальности «Прикладная информатика» и приобретение ими:
- знаний о типах сетевых атак, способах и методах обнаружения сетевых атак, программно-технических средствах обнаружения и предотвращения сетевых атак;
- умений обнаружения и предотвращения компьютерных атак, ;
- навыков конфигурирования программно-технических средств обнаружения и предотвращения сетевых атак.

2. Место учебной дисциплины в структуре ОП ВО

Учебная дисциплина "Системы обнаружения компьютерных атак" 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:

ПК-18	способностью управлять проектами по информатизации прикладных задач и созданию ИС предприятий и организаций

4. Общая трудоемкость дисциплины составляет

4 зачетных единиц (144 ак. ч.).

5. Образовательные технологии

В соответствии с требованиями федерального государственного образовательного стандарта высшего профессионального образования для реализации компетентностного подхода и с целью формирования и развития профессиональных навыков студентов по усмотрению преподавателя в учебном процессе могут быть использованы в различных сочетаниях активные и интерактивные формы проведения занятий, включая: Лекционные занятия. Информатизация образования обеспечивается с помощью средств новых информационных технологий - ЭВМ с соответствующим периферийным оборудованием; средства и устройства манипулирования аудиовизуальной информацией; системы машинной графики, программные комплексы (операционные системы, пакеты прикладных программ).Лабораторные занятия. Информатизация образования обеспечивается с помощью средств новых информационных технологий - ЭВМ с соответствующим периферийным оборудованием; виртуальные лабораторные работы. Самостоятельная работа. Дистанционное обучение - интернет-технология, которая обеспечивает студентов учебно-методическим материалом, размещенным на сайте академии, и предполагает интерактивное взаимодействие между преподавателем и студентами. Контроль самостоятельной работы. Использование тестовых заданий, размещенных в системе «Космос», что предполагает интерактивное взаимодействие между преподавателем и студентами..

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

РАЗДЕЛ 1
Раздел 1. Классификация сетевых атак

Снифферы пакетов, IP спуфинг, DoS и DDoS, Man in the Middle

РАЗДЕЛ 1
Раздел 1. Классификация сетевых атак
выполение КР

РАЗДЕЛ 2
Раздел 2. Принципы построения систем обнаружения вторжений (СОВ)

Классификация и архитектура СОВ. Существующие технологии обнаружения вторжений: обнаружение аномальной активности; сигнатурные методы; комплексные методы.

РАЗДЕЛ 2
Раздел 2. Принципы построения систем обнаружения вторжений (СОВ)
выполнение КР

РАЗДЕЛ 3
Раздел 3. Системы обнаружения компьютерных атак

Программные и программно-аппаратные системы обнаружения вторжений (IDS). Зарубежные и отечественные программные системы: Snort, Sourcefire IPS, McAfee Network Security Platform, Аргус, Ручей-М, Форпост. Программно-аппаратные IDS фирмы Cisco. Конфигурирование IDS.

РАЗДЕЛ 3
Раздел 3. Системы обнаружения компьютерных атак
защита ЛР выполнение КР(1)

РАЗДЕЛ 4
допуск к экзамену

РАЗДЕЛ 4
допуск к экзамену
защита КР

Экзамен

Экзамен
экзамен

Экзамен

Тема: Курсовая работа