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 Носиловский Евгений Антонович, к.ф.-м.н., доцент

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

«Криптографическая защита бизнес информации»

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 «Криптографическая защита бизнес информации» является формирование у обучающихся компетенций в соответствии с федеральными государственными образовательными стандартами по специальности «Прикладная информатика» и приобретение ими:
- знаний о шифровании с помощью симметричных и ассиметричных ключей;
- умений использовать математические методы в криптографии;
- навыков применения методов криптографической защиты бизнес информации.

2. Место учебной дисциплины в структуре ОП ВО

Учебная дисциплина "Криптографическая защита бизнес информации" 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-5	способностью исследовать применение различных научных подходов к автоматизации информационных процессов и информатизации предприятий и организаций

4. Общая трудоемкость дисциплины составляет

4 зачетные единицы (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. Математика криптографии.

Модульная арифметика, сравнения и матрицы.
Алгебраические структуры.
Простые числа и уравнения сравнения.

РАЗДЕЛ 1
Раздел 1. Математика криптографии.
О

РАЗДЕЛ 2
Раздел 2. Введение в основы современных шифров с симметричным ключом.

Современные блочные шифры. Современные шифры потока.
Стандарты шифрования DES и AES.

РАЗДЕЛ 2
Раздел 2. Введение в основы современных шифров с симметричным ключом.
ОК

РАЗДЕЛ 3
Раздел 3. Криптография с ассиметричным ключом

Криптографические системы RSA.
Криптосистемы Рабина и Эль-Гамаля.
Криптосистемы на основе метода эллиптических кривых.

РАЗДЕЛ 3
Раздел 3. Криптография с ассиметричным ключом
ОК

РАЗДЕЛ 4
Раздел 4. Некоторые вопросы криптографии

Целостность сообщения и установление подлинности сообщения.
Криптографические хэш-функции.
Цифровая подпись.

РАЗДЕЛ 4
Раздел 4. Некоторые вопросы криптографии
ОК

РАЗДЕЛ 5
Допуск к диф. зачёту

РАЗДЕЛ 5
Допуск к диф. зачёту
К

РАЗДЕЛ 6
Зачёт с оценкой

РАЗДЕЛ 6
Зачёт с оценкой
О

Дифференцированный зачет

РАЗДЕЛ 8
Контрольная работа