МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»

Кафедра «Вычислительные системы и сети»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

«Компьютерная безопасность»

Направление подготовки:	38.03.02 – Менеджмент
Профиль:	Транспортный бизнес и логистика
Квалификация выпускника:	Бакалавр
Форма обучения:	очная
Год начала подготовки	2018

1. Цели освоения учебной дисциплины

Целями освоения учебной дисциплины «Компьютерная безопасность» являются изучение студентами основных понятий информационной безопасности, изучение основных видов угроз информационной безопасности; получение представления об организации и принципах обеспечения информационной безопасности; знакомство с основами методов криптографического закрытия данных; получение навыков разработки политики безопасности предприятия.
Основными задачами дисциплины являются:
• освоение методов оценки степени угрозы информационной безопасности;
• изучение использования соответствующих методов защиты.;
• рассмотрение методов организации комплексной системы защиты информации;
• изучение студентами основных угроз информационной безопасности и методов защиты от них.

Дисциплина предназначена для получения знаний для решения следующих профессиональных задач (в соответствии с видами деятельности):

Организационно-управленческая деятельность:
• оценки степени угрозы информационной безопасности;
• участие в разработке организационно-технической документации (графиков работ, инструкций, планов, смет) и установленной отчетности по утвержденным формам.

Предпринимательская деятельность:
• безопасное использование глобальных компьютерных сетей;
• применение защищенной электронной коммерции;
• безопасное использование электронной почты;

2. Место учебной дисциплины в структуре ОП ВО

Учебная дисциплина "Компьютерная безопасность" 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:

ОПК-4	способностью осуществлять деловое общение и публичные выступления, вести переговоры, совещания, осуществлять деловую переписку и поддерживать электронные коммуникации
ОПК-7	способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
ПК-6	способностью участвовать в управлении проектом, программой внедрения технологических и продуктовых инноваций или программой организационных изменений

4. Общая трудоемкость дисциплины составляет

2 зачетные единицы (72 ак. ч.).

5. Образовательные технологии

Проведение занятий по дисциплине «Компьютерная безопасностьг» осуществляется в форме лекций и практических занятий. Лекции являются традиционными классически-лекционными с использованием презентаций. Практические занятия организованы с использованием технологий развивающего обучения. Оценка полученных знаний, умений и навыков основана на модульно-рейтинговой технологии. Фонды оценочных средств освоенных компетенций включают как вопросы теоретического характера для оценки знаний, так и задания практического содержания для оценки умений и навыков. .

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

РАЗДЕЛ 1
КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА

Работа с основной и дополнительной литературой [1],[2],[3], а также с периодическими изданиями на сайте http://elibrary.ru/

Тема: Классификация криптографических алгоритмов.

Классификация криптографических алгоритмов. Основные определения. Назначение шифрования. Принципы криптографического закрытия информации. Простые методы шифрования. Таблица Вижинера. Шифрование с открытым и закрытым ключами. Основные виды атак на криптоалгоритмы.

Тема: Симметричные криптоалгоритмы.Блочные и потоковые криптоалгоритмы. Алгоритм DES. Алгоритм 3DES. Алгоритм AES. Вопросы стойкости криптоалгоритмов. проблема распределения ключей. Достоинства и недостатки симметричного шифрования.

Симметричные криптоалгоритмы.Блочные и потоковые криптоалгоритмы. Алгоритм DES. Алгоритм 3DES. Алгоритм AES. Вопросы стойкости криптоалгоритмов. проблема распределения ключей. Достоинства и недостатки симметричного шифрования.

Тема: Асимметричные криптоалгоритмы. Алгоритм RSA. Алгоритм Диффи-Хэлмана. Электронно-цифровая подпись. Достоинства и недостатки асимметричного шифрования и область его применения.

Асимметричные криптоалгоритмы. Алгоритм RSA. Алгоритм Диффи-Хэлмана. Электронно-цифровая подпись. Достоинства и недостатки асимметричного шифрования и область его применения.

Контрольная работа

РАЗДЕЛ 2
ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА.

Работа с основной и дополнительной литературой [1],[2],[3], а также с периодическими изданиями на сайте http://elibrary.ru/

Тема: Аутентификация, авторизация и администрирование действий пользователей.

Аутентификация, авторизация и администрирование действий пользователей.

Тема: Основные принципы системы AAA. Методы аутентификации: пароли, PIN и биометрические данные. Авторизация. Accounting. Сервер AAA.

Основные принципы системы AAA. Методы аутентификации: пароли, PIN и биометрические данные. Авторизация. Accounting. Сервер AAA.

Тема: Фильтрация трафика. Списки доступа. Инспекция трафика. Традиционный межсетевой экран.

Фильтрация трафика. Списки доступа. Инспекция трафика. Традиционный межсетевой экран.

РАЗДЕЛ 3
ЗАЩИТА ИНФОРМАЦИИ В ГЛОБАЛЬНОЙ СЕТИ.

Работа с основной и дополнительной литературой [1],[2],[3], а также с периодическими изданиями на сайте http://elibrary.ru/

Тема: Защита http-трафика. Характерные угрозы. Защищенный протокол httpd.

Защита http-трафика. Характерные угрозы. Защищенный протокол httpd.

Тема: Цифровые сертификаты.. Виртуальная частная сеть.

Цифровые сертификаты.. Виртуальная частная сеть.

Контрольная работа

Тема: Туннелирование трафика. Виртуальные каналы. Архитектура VPN. Стандарты IPsec.

Туннелирование трафика. Виртуальные каналы. Архитектура VPN. Стандарты IPsec.