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

«Техническая защита информации»

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

Целями освоения учебной дисциплины «Техническая защита информации» являются формирование компетенции по основным разделам теоретических и практических основ организации средств защиты информации, дать необходимые навыки по использованию средств защиты информации в компьютерных системах и овладению методами решения соответствующих задач.

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

Проектно-технологическая деятельность:
• сбор и анализ исходных данных для обеспечения информационной безопасности с помощью средств технической защиты информации;
• разработка проектной и рабочей документации, оформление отчетов по законченным проектно-конструкторским работам;
• контроль соответствия разрабатываемых проектов и технической документации стандартам, техническим условиям и другим нормативным документам.

Экспериментально-исследовательская деятельность:
• анализ научно-технической информации, отечественного и зарубежного опыта по тематике исследования;
• подготовка данных и составление обзоров, рефератов, отчетов, научных публикаций и докладов на международных конференциях и семинарах, участие во внедрении результатов исследований и разработок.

Эксплуатационная деятельность:
• 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;
Организационно-управленческая деятельность
- организация работы коллектива исполнителей, принятие управленческих решений в условиях спектра мнений, определение порядка выполнения работ;
- поиск рациональных решений при разработке средств защиты информации с учетом требований качества, надежности и стоимости, а также сроков исполнения;
- осуществление правового, организационного и технического обеспечения защиты информации;

2. Место учебной дисциплины в структуре ОП ВО

Учебная дисциплина "Техническая защита информации" 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:

ПК-3	способностью администрировать подсистемы информационной безопасности объекта защиты
ПК-5	способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации
ПК-6	способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации
ПК-12	способностью принимать участие в проведении экспериментальных исследований системы защиты информации

4. Общая трудоемкость дисциплины составляет

3 зачетные единицы (108 ак. ч.).

5. Образовательные технологии

Преподавание дисциплины «Техническая защита информации» осуществляется в форме лекций, лабораторных занятий и выполнения курсового проекта.Лекции проводятся в традиционной классно-урочной организационной форме в объеме 12 часов, по типу управления познавательной деятельностью на 100 % являются традиционными классически-лекционными (объяснительно-иллюстративными).Лабораторный практикум (28 часов) проводится с использованием интерактивных (диалоговых) технологий, в том числе электронный практикум (решение проблемных поставленных задач с помощью современной вычислительной техники и исследование моделей); технологий, основанных на коллективных способах обучения. Самостоятельная работа студента организована с использованием традиционных видов работы. К традиционным видам работы (41 час) относится отработка лекционного материала и отработка отдельных тем по учебным пособиям.Оценка полученных знаний, умений и навыков основана на модульно-рейтинговой технологии. Весь курс разбит на 6 разделов, представляющих собой логически завершенный объем учебной информации. Фонды оценочных средств освоенных компетенций включают как вопросы теоретического характера для оценки знаний, так и задания практического содержания (решение конкретных задач, работа с данными) для оценки умений и навыков. 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
РАЗДЕЛ 1. ВВЕДЕНИЕ В ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ

Тема 1.1. Основные понятия.
Введение. Информация. и защита данных. Конфиденциальность информации. Целостность информации. Доступность информации. Служебная информация. Личные данные.

Тема 1.2. Государственные структуры, отвечающие за защиту данных. Определение служебной тайны.
Законодательство РФ в области информационной безопасности. Информационная безопасность коммерческой структуры. Типовой набор должностей, связанных с защитой данных на предприятии.;

Тема 1.3. Международные стандартизирующие организации. Стандарты РФ в области информационной безопасности..

РАЗДЕЛ 2
РАЗДЕЛ 2. УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
Выполнение лаб.работ 20%

Тема 2.1. Природа возникновения угроз. Классификация угроз по преднамеренности проявления. Классификация по источнику угрозы. Классификация по степени воздействия на информационную систему. По способам доступа к ресурсам информационной системы.

Тема 2.2 Угрозы безопасности информационной системы.

Тема 2.3. Методы противодействия несанкционированному доступу, сетевой разведке и DOS-атакам.

РАЗДЕЛ 3
РАЗДЕЛ 3. ПОЛИТИКА БЕЗОПАСНОСТИ

Тема 3.1. Структура политики безопасности.

Тема 3.2. Базовая политика безопасности.

Тема 3.3 Специализированные политики безопасности.

РАЗДЕЛ 4
РАЗДЕЛ 4. КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА

Тема 4.1. 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 4.2. Симметричные криптоалгоритмы.Блочные и потоковые криптоалгоритмы.

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

Тема 4.3. Асимметричные криптоалгоритмы. Алгоритм RSA. Алгоритм Диффи-Хэлмана. Электронно-цифровая подпись. Достоинства и недостатки асимметричного шифрования и область его применения.

РАЗДЕЛ 5
РАЗДЕЛ 5. ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА.

Тема 5.1. Аутентификация, авторизация и администрирование действий пользователей.

Тема 5.2. Основные принципы системы AAA. Методы аутентификации: пароли, PIN и биометрические данные. Авторизация. Accounting. Сервер AAA.

Тема 5.3. Фильтрация трафика. Списки доступа. Инспекция трафика. Традиционный межсетевой экран.

РАЗДЕЛ 6
РАЗДЕЛ 6. ЗАЩИТА ИНФОРМАЦИИ В ГЛОБАЛЬНОЙ СЕТИ.
Выполнение лаб.работ 80%

Тема 6.1. Защита http-трафика. Характерные угрозы. Защищенный протокол httpd.

Тема 6.2. Цифровые сертификаты.. Виртуальная частная сеть.

Тема 6.3. Туннелирование трафика. Виртуальные каналы. Архитектура VPN. Стандарты IPsec.

РАЗДЕЛ 7
Итоговая информация