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

«Основы информационной безопасности »

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 «Основы информационной безопасности» 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):

Проектно-технологическая деятельность:
• сбор и анализ исходных данных для оценки потенциальных угроз информационной безопасности и для решения задачи 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:
• участие в работе малых групп исполнителей;
• участие в разработке организационно-технической документации (графиков работ, инструкций, планов, смет) и установленной отчетности по утвержденным формам.
Организационно-управленческая деятельность:
• организация работы малых групп исполнителей;
• участие в разработке организационно-технической документации (графиков работ, инструкций, планов, смет) и установленной отчетности по утвержденным формам.

2. Место учебной дисциплины в структуре ОП ВО

Учебная дисциплина "Основы информационной безопасности " 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:

ОК-5	способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики

4. Общая трудоемкость дисциплины составляет

3 зачетные единицы (108 ак. ч.).

5. Образовательные технологии

Преподавание дисциплины «Основы информационной безопасности» осуществляется в форме лекций, лабораторных занятий и выполнения курсового проекта.Лекции проводятся в традиционной классно-урочной организационной форме в объеме 32 часа, по типу управления познавательной деятельностью на 100 % являются традиционными классически-лекционными (объяснительно-иллюстративными).Практические занятия (18 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 (53 часа) 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
ВВЕДЕНИЕ В ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ

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

Тема: 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: Международные стандартизирующие организации.

РАЗДЕЛ 2
УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Тема: 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: Угрозы безопасности информационной системы и методы противодействия несанкционированному доступу, сетевой разведке и DOS-атакам.

РАЗДЕЛ 3
ПОЛИТИКА БЕЗОПАСНОСТИ

Тема: Структура политики безопасности
Выполнение и сдача лабораторной работы 20%

Тема: Базовая политика безопасности.

Тема: Специализированные политики безопасности

РАЗДЕЛ 4
КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА

Тема: 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.

Тема: Асимметричные криптоалгоритмы.
Выполнение и сдача лабораторной работы 80%

Тема: Асимметричные криптоалгоритмы.
Алгоритм RSA. Алгоритм Диффи-Хэлмана. Электронно-цифровая подпись. Достоинства

и недостатки асимметричного шифрования и область его применения.

РАЗДЕЛ 5
ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА.

Тема: Аутентификация, авторизация и администрирование действий пользователей. 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.

РАЗДЕЛ 6
ЗАЩИТА ИНФОРМАЦИИ В ГЛОБАЛЬНОЙ СЕТИ.

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

Тема: Цифровые сертификаты.. Виртуальная частная сеть.

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

РАЗДЕЛ 7
Итоговая аттестация