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

«Информационная безопасность»

Направление подготовки:	09.03.01 – Информатика и вычислительная техника
Профиль:	Вычислительные машины, комплексы, системы и сети
Квалификация выпускника:	Бакалавр
Форма обучения:	очная
Год начала подготовки	2018

1. Цели освоения учебной дисциплины

В соответствии с общими целями ФГОС ВПО по направлению «Информатика и вычислительная техника», целью дисциплины является изуче-ние студентами основных понятий информационной безопасности, изуче-ние 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.
Дисциплина предназначена для получения знаний для решения следующих профессиональных задач (в соответствии с видами деятельности):

Проектно-технологическая деятельность

• Применение современных инструментальных средств при разработке программного обеспечения.
• Применение Web-технологий при реализации удаленного доступа в системах клиент/сервер и распределенных вычислений.
• Использование стандартов и типовых методов контроля и оценки качества программной продукции.
• Участие в работах по автоматизации технологических процессов в ходе подготовки производства новой продукции.
• Освоение и применение современных программно-методических комплексов исследования и автоматизированного проектирования объектов профессиональной деятельности.
Научно-исследовательская деятельность

• Изучение научно-технической информации, отечественного и зарубежного опыта по тематике исследования.
• Математическое моделирование процессов и объектов на базе стандартных пакетов автоматизированного проектирования и исследований.
• Проведение экспериментов по заданной методике и анализ результатов.
• Проведение измерений и наблюдений, составление описания проводимых исследований, подготовка данных для составления обзоров, отчетов и научных публикаций.
• Составление отчета по выполненному заданию, участие во внедрении результатов исследований и разработок.

2. Место учебной дисциплины в структуре ОП ВО

Учебная дисциплина "Информационная 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-5	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-2	способностью разрабатывать компоненты аппаратно-программных

	комплексов и баз данных, используя современные инструментальные средства и технологии программирования

4. Общая трудоемкость дисциплины составляет

4 зачетные единицы (144 ак. ч.).

5. Образовательные технологии

Преподавание дисциплины «Информационная безопасность» осуществляется в форме лекций, лабораторных занятий и выполнения курсового проекта.Лекции проводятся в традиционной классно-урочной организационной форме в объеме 26 часов, по типу управления познавательной деятельностью на 100 % являются традиционными классически-лекционными (объяснительно-иллюстративными). Лабораторные работы организованы с использованием технологий развивающего обучения. Курс лабораторных работ (12 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 (39 часов) организована с использованием традиционных видов работы. К традиционным видам работы 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. .

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

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.
Угрозы безопасности информационной системы.
Сетевая разведка: Sniffing; Ping-sweep, сканирование портов. Несанкционированный

доступ: IP-spoofing; Man-in-the-middle; Подмена стороны. DOS-атака. DDOS-атака. Уязвимость программных приложений. Методы противодействия несанкционированному доступу, сетевой разведке и DOS-атакам.
Компьютерные вирусы. Троянские программы. Сетевые черви. Пути распространения вредоносного программного кода. Программы удаления вредоносного программного кода. Обновления безопасности. Антивирусные программы.

Тема: Природа возникновения угроз.
выполнение и защита лабораторных работ №1-2

РАЗДЕЛ 3
Политика безопасности

Тема: Структура политики безопасности.
Базовая политика безопасности. Специализированные политики безопасности. Процедуры безопасности. Уровни решений политики безопасности: верхний, средний и нижний. Область применения политики безопасности. Выработка позиции организации. Роль руководителей подразделений. Роль администраторов сетей. Роль администраторов сервисов. Роль пользователя информационной системы. Санкции.

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.
Симметричные криптоалгоритмы.Блочные и потоковые криптоалгоритмы. Алгоритм DES. Алгоритм 3DES. Алгоритм AES. Вопросы стойкости криптоалгоритмов. проблема распределения ключей. Достоинства и недостатки симметричного шифрования.
Асимметричные криптоалгоритмы.Алгоритм RSA. Алгоритм ДиффиХэлмана. Электронно-цифровая подпись. Достоинства и недостатки асимметричного шифрования и об-ласть 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.
Фильтрация трафика. Списки доступа. Инспекция трафика. Традиционный межсетевой экран. Технология Zone-based farewall. Основные схемы применения межсетевых экранов.
Методы анализа сетевой информации. Сигнатуры. Системы обнаружения вторжений (IDS). Системы предотвращения вторжений (IPS).

Тема: Аутентификация, авторизация и администрирование действий пользователей.
выполнение лаб.работ

РАЗДЕЛ 6
Защита информации в глобальной сети.

Тема: Защита http-трафика.
Характерные угрозы. Защищенный протокол httpd. Цифровые сертификаты.Виртуальная частная сеть.
Туннелирование трафика. Виртуальные каналы. Архитектура VPN. Стандарты IPsec.

РАЗДЕЛ 7
Итоговая аттестация