

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

«Методы и средства обеспечения информационной безопасности»

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

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 "Методы и средства обеспечения информационной безопасности" 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 «Методы и средства обеспечения информационной безопасности» 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 заверченный 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 управление информационной безопасностью

Тема: Основные понятия.

Управление информационными рисками

Международные стандартизирующие организации и стандарты в области управления информационной безопасностью.

РАЗДЕЛ 2

Основные функции систем управления информационной безопасностью

Тема: Понятие систем управления информационной безопасностью (СУИБ)

Функции систем управления информационной безопасностью.

Выявление и анализ рисков информационной безопасности; планирование и практическая реализация процессов, направленных на минимизацию рисков ИБ; контролирование этих процессов; внесение в процессы минимизации информационных рисков необходимых корректировок.

Тема: Понятие систем управления информационной безопасностью (СУИБ)

выполнение и защита лабораторных работ №1-2

РАЗДЕЛ 3

Принципы качественного управления информационной безопасностью

Тема: Качественное управление информационной безопасностью.

Комплексный подход; рискообразующие факторы; согласованность с бизнес-задачами и

стратегией предприятия; уровень управляемости; адекватность используемой и генерируемой информации; эффективность СУИБ как баланс между возможностями, производительностью и издержками; непрерывность управления; процессный подход.

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 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.

Фильтрация трафика. Списки доступа. Инспекция трафика. Традиционный межсетевой экран. Технология Zone-based firewall. Основные схемы применения межсетевых экранов. Методы анализа сетевой информации. Сигнатуры. Системы обнаружения вторжений (IDS). Системы предотвращения вторжений (IPS).

РАЗДЕЛ 6

Иерархическая организация процессов управления информационной безопасностью

Тема: Иерархия процессов управления информационной безопасностью.

Замкнутый жизненный цикл системы управления информационной безопасностью.

Системный подход к созданию системы управления информационной безопасностью.

РАЗДЕЛ 7

Итоговая аттестация