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

«Теоретические основы компьютерной 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 «Теоретические основы компьютерной безопасности» являются - освоение студентами базовых методов и средств защиты компьютерной информации (организационных, технических, программных), ознакомление с законодательством и стандартами в этой области.
Студенты должны изучить теоретические основы компьютерной безопасности и уметь применять теорию на практике.
Основными задачами дисциплины являются:
? Изучение методов и средств защиты при работе в Internet.
? Ознакомление с процессом управления доступом к ресурсам.
? Изучение современных криптосистем,
? Изучение информационного процесса управления криптографическими ключами
? Изучение алгоритмов ЭП и хеш-функций.
? Изучение политики безопасности.
? Изучение основ проектирования систем защиты информации.

Дисциплина формирует знания и умения для решения следующих профессиональных задач (в соответствии с видами профессиональной деятельности):
Эксплуатационная:
- 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;
Проектно-технологическая:
- сбор и анализ исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности;
- проведение проектных расчетов элементов систем обеспечения информационной безопасности;
- участие в разработке технологической и эксплуатационной документации;
- проведение предварительного технико-экономического обоснования проектных расчетов
Экспериментально-исследовательская деятельность:
- сбор, изучение научно-технической информации, отечественного и зарубежного опыта по тематике исследования;
- проведение экспериментов по заданной методике, обработка и анализ их результатов;
- проведение вычислительных экспериментов с использованием стандартных программных средств
Организационно-управленческая деятельность:
- осуществление организационно-правового обеспечения информационной безопасности объекта защиты;
- организация работы малых коллективов исполнителей;
- участие в совершенствовании системы управления информационной безопасностью;
- изучение и обобщение опыта работы других учреждений, организаций и предприятий в области защиты информации, в том числе информации ограниченного доступа;
- контроль эффективности реализации политики информационной безопасности объекта защиты.

2. Место учебной дисциплины в структуре ОП ВО

Учебная дисциплина "Теоретические основы компьютерной 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:

ОПК-2	способностью применять соответствующий математический аппарат для решения профессиональных задач
ПК-4	способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты
ПК-7	способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений

4. Общая трудоемкость дисциплины составляет

4 зачетные единицы (144 ак. ч.).

5. Образовательные технологии

Преподавание дисциплины «Теоретические основы компьютерной безопасности» осуществляется в форме лекций и лабораторных занятий. Лекции проводятся в традиционной классно-урочной организационной форме в объеме 28 часов, а также с использованием интерактивных (диалоговых) технологий по типу управления познавательной деятельностью (6 часов), являются классически-лекционными (объяснительно-иллюстративными).Лабораторные работы организованы с использованием технологий развивающего обучения. Курс лабораторных работ (14 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 (8 часов). Самостоятельная работа студента организована с использованием традиционных видов работы. К традиционным видам работы (57 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 13 разделов, представляющих собой логически завершенный объем учебной информации. Фонды оценочных средств освоенных компетенций включают вопросы теоретического характера 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 дисциплину.
1. Введение (основные понятия и определения).
2. Характеристики угроз, служб и механизмов безопасности (виды; взаимосвязь между службами и реализующими их механизмами).

РАЗДЕЛ 2
Правовые и организационные методы защиты информации.
методы и средства защиты (технические, программные, физические, организационные). компьютерной информации.
2. Законодательные меры защиты информации (нормативные правовые акты РФ в области защиты информации).
3. Существующие стандарты (оценочные стандарты и технические спецификации; организации-разработчики стандартов).

РАЗДЕЛ 3
Угрозы безопасности информации в компьютерных системах.
. Классификация угроз (пути их реализации; комплекс требований к системе компьютерной безопасности).
2. Основные способы и каналы утечки информации (преодоление программных средств защиты; способы несанкционированного доступа).

РАЗДЕЛ 4
Аппаратно-программные средства защиты информации.
(выполнение и защита лабораторных работ №1-№2

РАЗДЕЛ 4
Аппаратно-программные средства защиты информации.
Основные средства защиты компьютерной информации и их функции (Zecurion Zgate; Secret Disk; КриптоПро CSP; другие разработки).
2. Уровни защиты информации (в эталонной модели OSI и в реальных системах; понятие архитектуры систем защиты информации).
3. Средства шифрования (защита от изменения потока сообщений и прерывания передачи; защита от навязывания ложных сообщений в каналы связи компьютерной

РАЗДЕЛ 5
Криптографические методы защиты информации.
защиты информации (шифры; особенности реализации методов криптозащиты).
2. Криптоаналитические атаки (виды; противодействия).

РАЗДЕЛ 6
Современные симметричные криптосистемы.
. Стандарты шифрования данных (алгоритм шифрования данных DES; Triple DES; AES; алгоритм Ривеста).
2. Российский стандарт крипто- и имитозащиты сообщений (режимы простой замены, гаммирования, гаммирования с обратной связью).

РАЗДЕЛ 7
Ассиметричные криптосистемы.
. Концепция криптосистемы с открытым ключом.

2. Криптосистема шифрования данных RSA.
3. Схемы шифрования (Полига-Хеллмана; Эль Гамаля; комбинированный метод шифрования).

РАЗДЕЛ 8
. Криптографические ключи.
Управление криптографическими ключами (виды ключей; процедуры управления ключами);
2. Генерация ключей (средства генерации случайных значений ключей; ANSI X 9.17).
3. Хранение ключей (устройства хранения закрытого ключа; спецификация TPM, криптопроцессоры).
4. Распределение ключей (задача распределения ключей; распределение ключей с участием ЦРК; построение протокола распределения ключей; SKIP).

РАЗДЕЛ 9
Управление доступом к ресурсам.
(выполнение и защита лабораторных работ №3-№4

РАЗДЕЛ 9
Управление доступом к ресурсам.
Требования, подходы и задачи управления доступом.
2. Модели доступа (механизмы управления доступом; идентификация и установление подлинности).
3. Проверка полномочий субъектов на доступ к ресурсам (регистрация обращений к защищаемым ресурсам; реагирование на несанкционированные действия).

РАЗДЕЛ 10
Электронная подпись.
. Проблема аутентификации данных.
2. Однонаправленные хэш-функции (использование в ЭП; стандарты хэш-функций).
3. Алгоритмы электронной подписи (назначение и виды, классификация, подделка ЭП).
4. Подписи с дополнительными функциональными свойствами (слепая ЭП, быстрая, неоспоримая).

РАЗДЕЛ 11
Методы и средства защиты при работе в Internet.
. Способы защиты сетей (сетевые атаки и методы противодействия; связь между характеристиками развития вирусной атаки и сетевой структурой).
2. Межсетевые экраны (особенности функционирования; основные компоненты; схемы сетевой защиты на базе межсетевых экранов; программные методы защиты).

РАЗДЕЛ 12
Проектирование систем защиты информации.
. Основы политики безопасности (понятие политики безопасности; реализация политики безопасности; модели безопасности).
2. Проектирование и реализация системы защиты информации (анализ объекта защиты; этапы проектирования и реализации системы; работы по созданию и сопровождению системы; архитектура системы защиты).

РАЗДЕЛ 13
Перспективы развития компьютерной безопасности
1. Перспективные направления исследований в области компьютерной безопасности.
2. Центры компьютерной безопасности.

РАЗДЕЛ 14
итоговая аттестация