МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ
Ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования
«Московский технический университет связи и информатики»
(МТУСИ)

Утверждена
решением совета факультета РиТ
от 17.09.2020, протокол №1,
Председатель совета факультета РиТ
_____ А.В.Пестряков

ПРОГРАММА ВСТУПИТЕЛЬНЫХ ИСПЫТАНИЙ В МАГИСТРАТУРУ

по направлению

11.04.02 «Инфокоммуникационные технологии и системы связи. Безопасность и программная защита инфокоммуникаций»

Москва 2020

1 ЦЕЛЬ И ЗАДАЧИ ВСТУПИТЕЛЬНЫХ ИСПЫТАНИЙ

Вступительные испытания предназначены для определения практической и теоретической подготовленности бакалавра и проводятся с целью определения соответствия знаний, умений и навыков студентов и проведения отбора среди лиц, желающих освоить программу подготовки магистра по направлению 11.04.02 «Инфокоммуникационные технологии и системы связи»

2 ВСТУПИТЕЛЬНЫЕ ИСПЫТАНИЯ

Все вступительные испытания оцениваются по 100-балльной шкале. Минимальный балл, позволяющий участвовать в конкурсе на зачисление – 30 баллов. Полученные на вступительных испытаниях результаты ниже 30 баллов являются неудовлетворительными и не позволяют поступающему участвовать в конкурсе на зачисление на бюджетные места и места по договору об оказании платных образовательных услуг.

Учет индивидуальных достижений поступающих при приеме на обучение представлен в Правилах приема в ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования «Московский технический университет связи и информатики» для поступающих на обучение по образовательным программам высшего образования – программам магистратуры в 2021 году.

На вступительном экзамене претенденту предлагается задание, состоящее из тестов, включающих в себя разделы области сетевых технологий, теории информационной безопасности и методов защиты информации, а также задачи по криптографии, отражающих основные квалификационные требования, предъявляемые к бакалавру (специалисту) для решения профессиональных задач. Экзаменационный билет состоит из 7 тестовых вопросов по каждому из двух разделов и задача по тематике третьего раздела. Каждый из 14 тестовых вопроса оценивается 5 баллами, задача по криптографии – 30 баллов. Максимальный балл – 100.

СОДЕРЖАНИЕ ПРОГРАММЫ ВСТУПИТЕЛЬНОГО ЭКЗАМЕНА

Сетевые технологии

Топологии и классификации сетей. Модель OSI. Кодирование информации на физическом уровне. Методы доступа к физической среде. труктура Ethernet-фрейма. Технология VLAN. MAC и IP-адресация. Протокол ARP. Маска подсети, IP-планирование сетей. Реальные и приватные IP-адресация. Назначение и структура полей IP/TCP/UDP-пакетов. Протоколы TCP и UDP. Маршрутизация и трансляция IP-адресов. Протокол Spanning Tree. Сетевые службы и сервисы DNS, DHCP и SNMP. Идентификация и разрешение сетевых проблем.

Теория информационной безопасности и методология защиты инфокоммуникаций

Информационная безопасность. Научная терминология. Базовые понятия. Концепция информационной безопасности России. Стандартизация в области информационной безопасности. Базовые архитектуры и услуги обеспечения безопасности инфокоммуникаций. Методы и средства защиты информации. Методы и модели оценки

защищенности (уязвимости) инфокоммуникаций. Анализ и управление риском в обеспечении информационной безопасности. Методы оптимизации в задачах обеспечения информационной безопасности.

Криптографические методы и средства обеспечения информационной безопасности инфокоммуникаций

Симметричные криптографические системы обеспечения информационной безопасности. Асимметричные криптографические системы обеспечения информационной безопасности. Электронная цифровая подпись в инфокоммуникациях. Методы и средства управления криптографическими ключами. Методы и средства реализации криптографически защищенных информационных систем.

Образец задания для экзамена для поступающих в магистратуру на факультет Радио и Телевидение по направлению 11.04.02 «Инфокоммуникационные технологии и системы связи. Безопасность и программная защита инфокоммуникаций»

1. **В модели Взаимодействия открытых систем (модель BOC или OSI) выделяются**
   1) 3 уровня
   2) 4 уровня
   3) 6 уровней
   4) 7 уровней
   5) 8 уровней

2. **В стеке TCP/IP выделяется**
   1) 3 уровня
   2) 4 уровня
   3) 6 уровней
   4) 7 уровней
   5) 8 уровней

3. **Технологией множественного доступа к общей передающей среде (каналу) является (*более одного правильного варианта ответа)*:**
   1) Ethernet
   2) CSMA/CD
   3) CSMA/CA
   4) FibreChannel

4. **Маршрутизатор (router) выполняет операции**
   1) коммутации пакетов (switching)
   2) продвижения пакетов (forwarding)
   3) пересылку пакетов в выходные порты в соответствие с маршрутной таблицей (routing)
   4) логистики пакетов (logistcs)
   5) разделения пакетов (separation)

5. Стандартизирующей организацией в области сетевых технологий :
   1) ITU

2) ISO
3) IEEE
4) EIA
5) TIA

6. Отличие между заголовками пакетов в протоколах IPv4 и IPv6 заключается в (*более одного правильного варианта ответа)*:

1) Наличие поля «Версия» в IPv4

2) Наличие поля «Класс трафика» в IPv6

3) Отсутствие поля «Контрольная сумма заголовка» в IPv6

4) Отсутствие поля «Адрес отправителя» в IPv6

5) Ничего из перечисленного выше

7. Протокол ICMP предназначен для:

1) передачи данных между сетевыми станциями (хостами)
2) передачи данных между прикладными процессами внутри сетевых станций
3) тестирования передачи данных
4) управления передачей данных
5) оповещения об ошибках передачи данных

8. Угрозы ИСПДн 1-го типа – это:

1) Непреднамеренные угрозы
2) Случайные угрозы
3) Преднамеренные угрозы
4) Угрозы, связанные с наличием недекларированных возможностей в системном ПО

9. Укажите угрозы конфиденциальности информации:

1) Потеря информации
2) Перехват информации
3) Утечка информации
4) Модификация информации
5) Копирование
6) Блокирование информации

10. В законе РФ «Об информации, информационных технологиях и о защите информации» дается основное определение информационно-телекоммуникационной сети. Это:

1) Сведения (сообщения, данные) независимо от формы их представления
2) Процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов
3)Технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники
4)Совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств

11. Межсетевой экран обеспечивает защиту инфокоммуникаций посредством:

1) Шифрования передаваемых данных
2) Авторизации пользователей АС
3) Фильтрации передаваемых данных
4) Обнаружения ошибок при передаче данных
5) Измерения первичных характеристик каналов связи

12. Какие основные способы разграничения доступа применяются в компьютерных системах:

1) дискреционный и мандатный.
2) по специальным спискам.
3) по группам пользователей и специальным разовым разрешениям.
4) многоуровневый

13. Назначение политики информационной безопасности организации. Это:

1) Обеспечение требуемого уровня безопасности обрабатываемой в телекоммуникационной системе информации при её проектировании, внедрении и эксплуатации
2) Организационные мероприятия, направленные на защиту информации
3) Совокупность правил, процедур, практических методов и руководящих принципов в области информационной безопасности, используемых организацией в своей деятельности
4) Определение целей и задач системы менеджмента информационной безопасности для формирования совокупности правил, требований и руководящих принципов в области информационной безопасности, которыми руководствуется организация в своей деятельности

14. Что представляют собой активные способы защиты информации от реализации технических каналов утечки информации

1) Установка на объектах инфокоммуникаций пространственного зашумления
2) Установка на объектах инфокоммуникаций линейного зашумления
3) Установка физических средств защиты информации

Задача:

С помощью алгоритма RSA зашифровать сообщение «КЛЮЧ» и добавить к нему электронную цифровую подпись (ЭЦП). Исходные данные: Для алгоритма RSA заданы взаимно простые числа P1=7; Q1=17, а также значение секретного ключа $K_{з1}$=11. Исходные данные для ЭЦП : P2=17; Q2=37; $K_{з2}$=19. Алгоритм вычисления Хэш-функции задан. Воспользоваться алфавитом русского языка.

При решении использовать следующие идентификаторы

<u>При шифровании:</u>

$\varphi(N)$ – функция Эйлера

K_O - *Открытый ключ*

M_i *–символ шифруемого сообщения*

C_i - *соответствующий код символа сообщения*

При нахождении Хэш функции

H_i – текущее(промежуточное) значение хжэщ функции

$m = H(M)$ искомое значение Хэш функции (дайджест) сообщения

При нахождении ЭЦП

S - искомая ЭЦП

Основная литература

1. Олифер В.Г., Олифер Н.А. Компьютерные сети: принципы, технологии, протоколы. Издание 5-ое. Учебник для ВУЗов. Питер СПб. 2019.- 992 с.
2. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сете: учеб. пособие. – М.: ИД «ФОРУМ»: ИНФРА-М, 2011. – 416 с.
3. Галатенко В.А. Основы информационной безопасности: учебное пособие /В.А.Галатенко. Под редакцией академика РАН В.Б.Бетелина – 4- е изд. –М.: Интернет-Университет Информационных технологий; БИНОМ. Лаборатория знаний, 2008.-205 с.
3. Лось А.Б. Криптографические методы защиты информации. Учебник для академического бакалавриата / А.Б. Лось; А.Ю.Нестеренко; М.И. Рожков. - М.:: Издательство Юрайт. 2016 – 473с .
4.Фороузан Бехроуз А. Криптография и безопасность сетей [Электронный ресурс]: учебное пособие/ Фороузан Бехроуз А.— Электрон. текстовые данные.— Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование, 2017.— 782 c.— Режим доступа: http://www.iprbookshop.ru/72337.html.— ЭБС «IPRbooks»

Дополнительная литература

1. Гатчин Ю.А., Сухостат В.В., Куракин А.С., Донецкая Ю.В. Теория информационной безопасности и методология защиты информации – 2-е изд., испр. и доп. – СПб: Университет ИТМО, 2018. – 100 с.
2. Басалова Г.В. Основы криптографии [Электронный ресурс]/ Басалова Г.В.— Элек-трон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 282 c.— Режим доступа: http://www.iprbookshop.ru/52158.— ЭБС «IPRbooks»
3. Т. Паркер, К. Сиян. TCP/IP. Для профессионалов. 3-е издание – издательский дом «Питер», 2003г.