Федеральное государственное образовательное бюджетное учреждение высшего образования
«ФИНАНСОВЫЙ УНИВЕРСИТЕТ ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»

Кафедра «Информационная безопасность»

УТВЕРЖДАЮ

Ректор Финуниверситета

_____М.А. Эскиндаров

«____» _____ 2016 г.

«ЗАЩИТА ИНФОРМАЦИОННЫХ ПРОЦЕССОВ В КОМПЬЮТЕРНЫХ СИСТЕМАХ»

Программа вступительного испытания

Для поступающих на обучение по программам бакалавриата по индивидуальному учебному плану лиц, имеющих соответствующее среднее профессиональное образование

Одобрено на заседании
Ученого совета Факультета
анализа рисков и экономической безопасности
(протокол № 30 от 18 октября 2016 г.)

Москва 2016

1. Содержание

Тема 1. Законодательные аспекты информационных технологий.

Теоретические основы защиты информации. Проблемы защиты информации в компьютерных системах. Терминология. Основные средства защиты информации в современных компьютерных системах и сетях. Основные задачи обеспечения безопасности информации в компьютерных сетях. Основные понятия криптографии. Требования к криптосистемам.

Законодательство РФ в области информационной безопасности. Информация как объект юридической и физической защиты. Государственные информационные ресурсы. Защита государственной тайны как особого вида защищаемой информации. Защита конфиденциальной информации, в том числе интеллектуальной собственности и коммерческой тайны. Нормативно-правовая база защиты компьютерных сетей от несанкционированного доступа. Компьютерные преступления и особенности их расследования.

Тема 2. Криптографические методы.

Основные понятия и определения. Понятие криптографических протоколов. Основные типы протоколов. Классы преобразований: подстановки, перестановки, гаммирование, блочные шифры. Симметричная криптография. Асимметричная криптография. Цифровой дайджест и хэш-функция. Подстановочные и перестановочные шифры. Шифры Цезаря, Виженера, Вернома. Нераскрываемость шифра Вернома.

Тема 3. Симметричные криптографические системы.

Стандарты шифрования DES, ГОСТ 28147-89: алгоритм, скорость работы на различных платформах, режимы пользования, основные результаты по анализу стойкости. Блочные алгоритмы. Алгоритм Blowfish. Потоковые алгоритмы. Алгоритм PKZIP. Теоретическая и практическая стойкость.

Тема 4. Асимметричные криптографические системы.

Системы с открытым ключом. Алгоритм шифрования RSA. Вычислительные аспекты реализации алгоритма RSA. Вопросы стойкости. Криптосистема Эль-Гамаля. Криптосистемы на основе эллиптических уравнений.

Тема 5. Задача обмена ключами

Алгоритм Диффи-Хеллмана. Протоколы обмена ключами на основе алгоритма Диффи-Хеллмана: двусторонний и многосторонний протокол.

Тема 6. Цифровая электронная подпись

Проблема аутентификации данных и электронная цифровая подпись. Однонаправленные хэш-функции. Алгоритм безопасного хэширования SHA. Однонаправленные хэш-функции на основе симметричных блочных алгоритмов. Отечественный стандарт хэш-функции. Электронная подпись на основе алгоритма RSA. Алгоритм цифровой подписи Эль-Гамаля (EGSA). Алгоритм цифровой подписи DSA. Отечественный стандарт цифровой подписи.

Тема 7. Безопасность современных сетевых технологий

Способы несанкционированного доступа к информации в компьютерных сетях. Классификация способов несанкционированного доступа и жизненный цикл атак. Способы противодействия несанкционированному межсетевому доступу. Функции межсетевого экранирования. Особенности межсетевого экранирования на различных уровнях модели OSI.

Режим функционирования межсетевых экранов и их основные компоненты. Маршрутизаторы. Шлюзы сетевого уровня. Основные схемы сетевой защиты на базе межсетевых экранов. Применение межсетевых экранов для организации виртуальных корпоративных сетей. Критерии

оценки межсетевых экранов. Построение защищенных виртуальных сетей. Способы создания защищенных виртуальных каналов. Обзор протоколов.

Тема 8. Безопасность в открытых сетях.

Инфраструктура на основе криптографии с открытыми ключами (ИОК). Цифровые сертификаты. Управление цифровыми сертификатами. Компоненты ИОК и их функции. Центр Сертификации. Центр Регистрации. Конечные пользователи. Сетевой справочник. Электронная почта и документооборот. Web приложения. Стандарты в области ИОК. Стандарты PKIX. Стандарты, основанные на ИОК (S/MIME, SSL и TLS, SET, IPSEC). Управление ключами.

Тема 9. Методы и средства встраивания скрытой служебной информации для управления правами доступа к информационным ресурсам.

Понятие стеганографии. Задача встраивания скрытой служебной информации (цифровых водяных знаков) в аудио и видеосигналы. Основные методы и алгоритмы встраивания и обнаружения водяных знаков. Встраивание водяных знаков и сжатие информации. Виды атак на информационные ресурсы, содержащие водяные знаки.

Перспективы обеспечения защиты информационных процессов в компьютерных системах. Шифрование сообщений и больших потоков данных. Шифрование, кодирование и сжатие информации. Реализация криптографических методов в компьютерных сетях.

2. Учебно-методическое и информационное обеспечение

Рекомендуемая литература

1. Жук А.П., Жук Е.П., Лепешкин О.М., Тимошкин А.И. Защита информации: Учебное пособие. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. - 392 с. Znanium.com.

2. Хорев П.Б. Программно-аппаратная защита информации: Учебное пособие. - 2-е изд., испр. и доп. - М.: Форум: НИЦ ИНФРА-М, 2015. - 352 с. Znanium.com.

3. Гришина Н.В. Информационная безопасность предприятия: Учебное пособие. - 2-е изд., доп. - М.: Форум: НИЦ ИНФРА-М, 2015. - 240с. Znanium.com.

4. Бабаш А.В. Криптографические методы защиты информации. Том 3: Учебно-методическое пособие. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2014. - 216 с. Znanium.com.

Дополнительная литература:

1. Васильков А.В., Васильков И.А. Безопасность и управление доступом в информационных системах: Учебное пособие. - М.: Форум: НИЦ ИНФРА-М, 2013. - 368 с. Znanium.com.

2. Баранова, Е. К. Основы информатики и защиты информации: Учебное пособие. - М. : РИОР : ИНФРА-М, 2013. - 183 с. Znanium.com.

3. Куняев Н.Н. Конфиденциальное делопроизводство и защищенный электронный документооборот: Учебник. - М.: Логос, 2011. - 452 с. Znanium.com.

4. Жданов О.Н. Методика выбора ключевой информации для алгоритма блочного шифрования: Монография. - М.: НИЦ ИНФРА-М, 2013. - 88 с. Znanium.com.

5. Ищейнов В.Я., Мецатунян М.В. Основные положения информационной безопасности: Учебное пособие. - М.: Форум, НИЦ ИНФРА-М, 2015. - 208 с. Znanium.com.

Программное обеспечение и Интернет-ресурсы

1. Офисные приложения.
2. Текстовый редактор (NotePad, WordPad).
3. ru.wikipedia.org – википедия.
4. www.rsl.ru – российская научная библиотека.