Федеральное государственное образовательное бюджетное
учреждение высшего образования
«Финансовый университет при Правительстве Российской Федерации»
«Методы и системы защиты информации, информационная безопасность»

Кафедра «Информационная безопасность»

«Методы и системы защиты информации, информационная безопасность»

Программа вступительного испытания для поступающих
на обучение по программе подготовки
научно-педагогических кадров в аспирантуре
Направление 10.06.01 «Информационная безопасность»

Москва 2017

Содержание программы

1. Общий теоретический раздел программы по направлению подготовки

Основные понятия и принципы теории информационной безопасности. Угрозы информационной безопасности. Виды информации, методы и средства обеспечения информационной безопасности. Методы нарушения конфиденциальности, целостности и доступности информации. Основы комплексного обеспечения информационной безопасности. Модели, стратегии и системы обеспечения информационной безопасности. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем. Лицензирование и сертификация в области защиты информации. Правовые основы защиты информации. Организационные основы защиты информации.

Локальные и глобальные вычислительные сети, типовые конфигурации, маршрутизация. Основные протоколы обмена данными в вычислительных сетях. Системы управления базами данных, реляционная, иерархическая и сетевая модели, распределенные БД. Деревья и графы, их представление в ЭВМ, обходы графов. Алгоритмы на графах, выделение компонент связности. Кратчайшие пути в графе, минимальный остов графа. Задача сортировки и основные алгоритмы сортировки. Поиск информации методом хеширования. Контрольно-испытательные и логико-аналитические методы анализа безопасности программ. Методы и средства хранения ключевой информации в ЭВМ. Защита программ от изучения, защита от изменения, контроль целостности. Защита от разрушающих программных воздействий.

2. Общий теоретический раздел по направленности (профилю) программы

Шифры замены и перестановки, их свойства, композиции шифров. Криптостойкость шифров, основные требования к шифрам. Теоретическая стойкость шифров, совершенные и идеальные шифры. Блоковые шифры. Потоковые шифры. Криптографические хеш-функции, их свойства и использование в криптографии. Методы получения случайных последовательностей, их использование в криптографии. Системы шифрования с открытыми ключами. Криптографические протоколы. Протоколы распределения ключей. Протоколы идентификации. Парольные системы разграничения доступа. Цифровая подпись. Стойкость систем с

открытыми ключами.

Методы решения систем линейных уравнений. Методы интерполяции. Методы численного интегрирования. Методы численного решения дифференциальных уравнений. Численные методы нахождения экстремумов функций. Элементы комбинаторики: перестановки, выборки, сочетания и размещения без повторений. Сочетания и размещения с повторениями, биномиальные коэффициенты, их свойства. Алгебра логики, формулы алгебры логики, высказывания и операции, построение формул. Случайные величины, математическое ожидание и дисперсия. Основные законы распределения случайной величины. Центральная предельная теорема. Цепи Маркова. Система массового обслуживания без очереди и с очередью.

3. Раздел программы по областям исследований (профилю кафедры)

Структура, классификация и основные характеристики технических каналов утечки информации. Побочные электромагнитные излучения и наводки. Классификация средств технической разведки, их возможности. Концепция и методы инженерно-технической защиты информации. Методы скрытия речевой информации в каналах связи. Методы обнаружения и локализации закладных устройств. Методы подавления опасных сигналов акустоэлектрических преобразователей. Методы подавления информативных сигналов в цепях заземления и электропитания. Виды контроля эффективности защиты информации. Методы расчета и инструментального контроля показателей защиты информации. Утечка информации от мощной офисной аппаратуры. Упрощенная методика определения дальности, на которой возможен перехват ПЭМИ. Утечка информации от вспомогательной аппаратуры и кабелей, проходящих через помещение. Привести примеры. Несанкционированный съем информации с помощью радиозакладок. Достоинства радиозакладок. Основные характеристики радиозакладок. Прослушивание информации от пассивных закладок. Достоинства и недостатки. Структурная схема полуактивного микрофона. Приемники информации с радиозакладок. Деконспирационные признаки радиозакладок. Методы пассивной защиты от утечки по электромагнитному каналу. Технические средства для поиска работающих радиозакладок. Поиск радиозакладок нелинейными радиолокаторами.

Нелинейные радиолокаторы с непрерывным режимом работы. Нелинейные радиолокаторы с импульсным режимом работы. Основы радиоэлектронной борьбы (РЭБ). Основы информационного противоборства. Проблемы деанонимизации в теневом интернете. Использование распределенных реестров и технологии блокчейн в задачах информационной безопасности

Шкала оценивания

Форма проведения вступительного испытания	Оценка по 100 балльной шкале
Письменная форма (компьютерное тестирование)	0-100 баллов

Рекомендуемая литература

Основная литература

1. Доктрина информационной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. №646
2. Крылов Г.О., Никитина В.Л. Понятийный аппарат информационной безопасности финансово-экономических систем. Энциклопедический словарь - М.: Финансовый университет, 2016.
3. Платонов В.В. Программно-аппаратные средства защиты информации: учебник для вузов. - М.: Издательский центр «Академия», 2013.
4. Сердюк В.А. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий: учебное пособие. - М.: Высшая школа экономики, 2011.
5. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. - М.: ДМК Пресс, 2012.
6. Фомичёв, В.М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты: учебник для академического бакалавриата / В. М. Фомичёв, Д. А. Мельников; под ред. В. М. Фомичёва. — М.: Юрайт, 2017.

7. Фомичёв, В. М. Криптографические методы защиты информации. В 2 ч. Часть 2. Системные и прикладные аспекты: учебник для академического бакалавриата / В. М. Фомичёв, Д. А. Мельников ; под ред. В. М. Фомичёва. — М.: Юрайт, 2016.
8. Актуальные проблемы информационного права. Учебник для вузов. ФГОС 3+. В.И. Авдийский, Г.О. Крылов и др.; под ред. И.Л. Бачило, М.А. Лапиной, М.: JUSTITIA, 2016

Дополнительная литература

1.Родичев Ю.А. Нормативная база и стандарты в области информационной безопасности. Учебное пособие. Стандарт третьего поколения. Учебник для вузов - Спб: Питер, 2017

2. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности: учебное пособие для вузов. - М.: Горячая линия-телеком, 2006.

3.Гатчин Ю.А., Климова Е.В. Основы информационной безопасности - Спб: СПбГУ ИТМО, 2009.

4. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. Технические средства и методы защиты информации: учебник для вузов. - М.: Машиностроение, 2009.

5. Ленков С.В., Перегудов Д.А. Методы и средства защиты информации. В 2-х томах. - М.: Арий, 2009 г.

6. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства. - М.: ДМК Пресс, 2008.

7. Сычев Ю.Н. Основы информационной безопасности. - М.: Евразийский открытый институт, 2010.

8. Крылов Г.О., Ларионова С.Л., Никитина В.Л. Базовые понятия информационной безопасности. Учебное пособие. – М.: РУСАЙНС, 2016