ПРОГРАММА ВСТУПИТЕЛЬНОГО ИСПЫТАНИЯ ДЛЯ НАПРАВЛЕНИЯ ПОДГОТОВКИ 10.04.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ («Информационная безопасность»)

Основы информационной безопасности

Информационная безопасность Российской Федерации. Угрозы информационной безопасности Российской Федерации. Доктрина информационной безопасности. Общие принципы защиты информации. Особенности программно-аппаратных закладок.

Безопасность (защищенность) автоматизированных систем. Обзор средств и методов информационной/компьютерной безопасности. Эпоха стандартизированной интегрированной программно-аппаратной защиты информации Trusted Platform Module (TPM). Классификация угроз. Методы нарушения секретности, целостности и доступности информации. Модели управления доступом. Контроль прав доступа.

Модели нарушителя и типичные атаки. Модель действий вероятного нарушителя и модель построения защиты. Классификация основных видов. Сетевая разведка. Оперативные средства и методы для нейтрализации атак.

Вредоносное программное обеспечение. Классификация вредоносных программ. Признаки присутствия вредоносного ПО. Методы защиты. Методы обнаружения. Способы внедрения. Примеры сетевых атак. Троянские программы, люки, эксплойты. Технологии самозащиты. Место и роль межсетевых экранов (МЭ) в обеспечении безопасности ресурсов АС. Возможности и ограничения антивирусных программ. Специализированные средства и методы выявления вредоносных программ.

Информационная война. Средства защиты и нападения. Информационная война и информационное оружие. Особенности технических средств информационной войны. Классификация средств защиты и нападения. Классификация электронных устройств перехвата информации, внедряемых в средства вычислительной техники. Средства СДВ (Силовое Деструктивное Воздействие).

Уничтожение информации. Необходимость уничтожения документов. Особенности удаления информации с электронных носителей. Политика уничтожения данных. Уничтожение конфиденциальной информации (плановое и экстренное). Следы в сети. Уникальные идентификаторы интернет-пользователей и электронные "отпечатки". Конфиденциальность в социальных сетях.

Организационное и правовое обеспечение информационной безопасности

Правовой режим защиты государственной тайны. Понятие правового режима защиты государственной тайны. Система нормативных правовых актов, регламентирующих обеспечение сохранности сведений, составляющих государственную тайну в РФ. Государственная тайна как особый вид защищаемой информации и ее характерные признаки. Принципы и механизмы отнесения сведений к государственной тайне, их засекречивания и рассекречивания. Органы защиты государственной тайны и их компетенция. Система контроля за состоянием защиты государственной тайны. Юридическая ответственность за нарушения правового режима защиты государственной тайны (уголовная, административная, дисциплинарная).

Правовые режимы защиты конфиденциальной информации. Понятие информации конфиденциального характера по российскому законодательству. Основные виды «конфиденциальной» информации: персональные данные, служебная тайна, коммерческая тайна, банковская тайна, профессиональная тайна, тайна следствия и судопроиз-

водства. Правовые режимы конфиденциальной информации: содержание и особенности. Основные требования, предъявляемые к организации защиты конфиденциальной информации. Юридическая ответственность за нарушения правовых режимов конфиденциальной информации (дисциплинарная, гражданско-правовая, административная и уголовная).

Государственное регулирование деятельности в области защиты информации. Понятие лицензирования по российскому законодательству. Виды деятельности, подлежащие лицензированию. Правовая регламентация лицензионной деятельности в области обеспечения информационной безопасности. Объекты лицензирования и участники лицензионных отношений в сфере защиты информации. Органы лицензирования и их полномочия. Организация лицензирования в сфере обеспечения информационной безопасности. Контроль за соблюдением лицензиатами условий ведения деятельности. Понятие подтверждения соответствия по российскому законодательству, формы подтверждения. Правовая регламентация сертификационной деятельности в области обеспечения информационной безопасности. Режимы сертификации. Объекты сертификационной деятельности (сертификации). Органы сертификации и их полномочия.

Программно-аппаратные средства защиты информации

Программно-аппаратные средства обеспечения информационной безопасности.

Основные понятия программно-аппаратной защиты. Защищенная автоматизированная система. Стандарты безопасности. Аппаратно-программные средства и методы защиты информации. Безопасное взаимодействие в компьютерной системе.

Защита программ и данных

Программно-аппаратные средства защиты ПЭВМ. Методы и средства ограничения доступа к компонентам ЭВМ. Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям. Методы и средства хранения ключевой информации. Защита от разрушающих программных воздействий. Защита от изменения и контроль целостности программ.

Защита информации в современных операционных системах

Типовая структура подсистемы безопасности операционных систем. Идентификация пользователей. Аутентификация. Защита обмена данных. Средства обеспечения безопасности в операционных системах. Домены безопасности. Критерии защищенности операционных систем. Механизмы и методы информационной безопасности.

Информационная безопасность базы данных. Механизмы обеспечения целостности и конфиденциальности СУБД

Средства обеспечения защиты информации в СУБД. Средства идентификации и аутентификации объектов баз данных, управление доступом. Средства контроля целостности информации, организация аудита. Типы контроля безопасности: потоковый, контроль вывода, контроль доступа. Многоуровневая защита. Модели безопасности, применяемые при построении защиты в СУБД.

Криптографическая защита в сетях Программно-аппаратные средства обеспечения информационной безопасности в вычислительных сетях. Протоколы аутентификации при удаленном доступе. Средства и методы обеспечения целостности и конфиденциальности. Защита серверов и рабочих станций. Средства защиты локальных сетей при подключении к Интернету. Защитные экраны. Защита виртуальных частных сетей

Методы и средства криптографической защиты информации

Основные задачи и понятия криптографии. Перечень угроз. Симметричное и асимметричное шифрование в задачах защиты информации. Шифры с открытым ключом и их использование. Классификация шифров. Модели шифров. Основные требования к шифрам. Простейшие криптографические протоколы.

Основные классы шифров и их свойства. Шифры перестановки. Разновидности шифров перестановки: маршрутные и геометрические перестановки. Элементы криптоанализа шифров перестановки. Поточные шифры замены. Шифры простой замены и их анализ. Многоалфавитные шифры замены. Шифры гаммирования и их анализ. Использование неравновероятной гаммы, повторное использование гаммы, криптоанализ шифра Виженера. Тесты У.Фридмана. Блочные шифры замены. Блочные шифры простой замены и особенности их анализа. Современные блочные шифры. Криптоалгоритмы ГОСТ-28147-89 и «Магма». Криптоалгоритмы AES, «Кузнечик».

Надёжность шифров. Основы теории К.Шеннона. Криптографическая стойкость шифров. Теоретически стойкие шифры. Шифры, совершенные при нападении на открытый текст. О теоретико-информационном подходе в криптографии. Энтропия и количество информации. “Ненадёжность шифра”, “ложные ключи” и “расстояние единственности”. Практически стойкие шифры. Вопросы имитозащиты. Имитостойкость шифров. Имитовставки. Коды аутентификации. Помехоустойчивость шифров. Понятие о помехоустойчивости шифра. Шифры, не размножающие искажений типа замены знаков. Шифры, не размножающие искажений типа пропуск-вставка знаков.

Методы синтеза и анализа криптографических алгоритмов с секретным ключом. Принципы построения криптографических алгоритмов. Принципы построения алгоритмов блочного шифрования. Выбор базовых преобразований. Режимы использования блочных шифров и их особенности. Принципы построения алгоритмов поточного шифрования. Режимы использования поточных шифров. Строение поточных шифрсистем. Типовые генераторы псевдослучайных последовательностей. Конгруэнтные генераторы.

Системы шифрования с открытым ключом. Шифрсистема RSA. Шифрсистема Эль-Гамаля. Шифрсистема на основе задачи об “укладке рюкзака”. Анализ шифрсистемы RSA. Практические аспекты использования шифрсистем с открытым ключом. Алгоритмы цифровых подписей. Цифровые подписи на основе шифрсистем с открытым ключом. Цифровая подпись Фиата-Шамира. Цифровая подпись Эль-Гамаля. Стандарты цифровой подписи. Алгоритмы идентификации. Протоколы типа запрос-ответ. Протоколы, использующие цифровую подпись. Протоколы с нулевым разглашением. Алгоритмы распределения ключей. Алгоритмы передачи ключей (с использованием и без использования цифровой подписи). Алгоритмы открытого распределения ключей. Алгоритмы предварительного распределения ключей.

Хеш-функции и их криптографические приложения. Общие сведения о хеш-функциях. Функция хэширования «Стрибог». Ключевые и бесключевые хеш-функции. Итеративные способы построения хеш-функций. Понятие о стойкости хеш-функции. Целостность данных и аутентификация источника данных.

Защита информации от утечки по техническим каналам

Системный подход к защите информации. Основные направления инженерно-технической защиты информации.

Информация как предмет защиты. Источники опасных сигналов. Характеристика технической разведки. Технические каналы утечки информации. Методы инженерно-технической защиты информации. Методы инженерной защиты и технической охраны объектов. Методы скрытия информации и ее носителей. Процессы подавления опасных сигналов.

Средства технической разведки. Средства инженерной защиты и технической охраны. Средства предотвращения утечки информации по техническим каналам.

Государственная система защиты информации. Контроль эффективности инженерно-технической защиты информации. Методические рекомендации по оценке эф-

фективности защиты информации.

Основы управления информационной безопасностью

Понятие информационной безопасности. Основные составляющие информационной безопасности. Угрозы информационной безопасности. Базовые вопросы управления информационной безопасностью. Цели и задачи управления информационной безопасностью.

Стандарты информационной безопасности. Серия стандартов ISO/IEC 27000 «Информационные технологии. Методы обеспечения безопасности». Стандарты на процессы управления информационной безопасности. Оценочные стандарты в информационной безопасности. Отраслевые стандарты в области управления информационной безопасностью. Сертификация системы информационной безопасности.

Системы управления информационной безопасностью (СУИБ). Понятие процессного подхода. Понятие СУИБ. Место СУИБ в рамках общей системы управления предприятием. Основные процессы СУИБ. Роль высшего руководства в организации системы управления информационной безопасностью. Политика информационной безопасности.

Оценка рисков информационной безопасности. Анализ рисков информационной безопасности. Инвентаризация активов. Понятие актива. Типы активов. Угрозы и уязвимости информационной безопасности. Оценка рисков информационной безопасности.

Процессы управления информационной безопасностью. Основные процессы СУИБ. Положение о применимости. Управление инцидентами информационной безопасности. Аудит информационной безопасности. Организация работы службы безопасности предприятия.

Обсуждена и одобрена на заседании предметной экзаменационной комиссии.

Одобрена на заседании приемной комиссии 26 мая 2023 г., протокол №2.

Минимальное количество баллов для вступительного испытания – ***40 баллов***.

Шкала оценивания вступительного испытания

Оценка	«Неудовлетворительно»	«Удовлетворительно»	«Хорошо»	«Отлично»
Баллы	0 – 39	40 – 70	71 – 84	85 – 100