Федеральное государственное бюджетное образовательное учреждение высшего образования
«ИВАНОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Шуйский филиал ИвГУ

Кафедра информационных систем и технологий

УТВЕРЖДЕНА
постановлением ученого совета
протокол № 6 от «31» августа 2018г.
председатель совета,
директор _____ А.А. Михайлов

**ПРОГРАММА**
**вступительного экзамена по специальной дисциплине**
**для направления подготовки высшего образования — подготовка кадров высшей квалификации по программам подготовки научно-педагогических кадров в аспирантуре**
**10.06.01 – Информационная безопасность**

Шуя – 2018

Программа составлена в соответствии с требованиями федеральных государственных образовательных стандартов высшего образования по программам специалитета и магистратуры.

## 1. Введение

Данная программа предназначена для сдачи вступительного экзамена по направлению подготовки 10.06.01 — Информационная безопасность, направленность «Методы и системы защиты информации, информационная безопасность».

Программа состоит из перечисления тем и их содержания, списка вопросов, литературы для подготовки к сдаче вступительного экзамена в аспирантуру.

**Цель экзамена** - выявить творческие интересы и реальную предрасположенность абитуриента к научно-исследовательской работе.

Экзаменующийся должен показать высокий уровень теоретической и профессиональной подготовки, знание основ теории, методов и средств защиты информации в современных системах ее обработки, путей и способов организации защиты с учетом текущего состояния и перспектив информатизации общества.

Содержание экзамена отражает современное состояние данного научно-технического направления и включает его важнейшие разделы, знание которых необходимо высококвалифицированному специалисту:

1. Научные основы защиты информации: основы информационной безопасности; теоретические основы компьютерной безопасности.
2. Основы современных информационных технологий: аппаратные средства вычислительной техники; методы программирования; языки программирования; электроника; системы и сети передачи информации.
3. Методы и средства обеспечения информационной безопасности: безопасность операционных систем; безопасность вычислительных сетей; безопасность систем баз данных; криптографические методы защиты информации; технические средства и методы защиты информации; программно-аппаратные средства обеспечения информационной безопасности.
4. Организационно-правовое обеспечение защиты информации: организационное обеспечение информационной безопасности; правовое обеспечение информационной безопасности.
5. Проектирование защищенных автоматизированных систем: комплексное обеспечение информационной безопасности автоматизированных систем; технология построения защищенных автоматизированных систем.

В программе приводится основная литература, знание которой требуется для сдачи экзамена. В соответствии с содержанием избранного направления поступающий должен продемонстрировать знания круга литературы и источников, знание актуальных проблем, связанных с темой будущей научно-исследовательской работы.

**Требования к уровню подготовки абитуриента.**

Поступающий в аспирантуру должен:

- обнаружить глубокие знания основ теории, методов и средств защиты информации в современных системах ее обработки, путей и способов организации защиты с учетом текущего состояния и перспектив информатизации общества;
- публикациях в периодической педагогической печати по вопросаморганизации защиты информации с учетом текущего состояния и перспектив информатизации общества;
- ориентироваться в проблематике дискуссий и критических взглядов современных ведущих ученых по затрагиваемым вопросам;
- уметь логично излагать материал;
- показать навыки владения понятийно-исследовательским аппаратом применительно к области специализации.

## 2. Процедура экзамена

Экзамен проводится в устной форме: с соискателем проводится устная беседа по материалам билета, включающего два вопроса из соответствующей программы. Продолжительность подготовки к ответу – 45 мин. Кроме того, после ответов на вопросы, проводится собеседование с целью выяснения предполагаемых направлений будущего диссертационного исследования.

Вступительные испытания оцениваются по 100-балльной шкале: ответ на каждый вопрос - 50 баллов максимум.

Критерии оценки:

41 - 50 баллов - дан полный, развернутый ответ на поставленный вопрос с использованием разных источников информации, доказательно раскрыты основные положения вопроса; в ответе прослеживается четкая структура, логическая последовательность, отражающая сущность раскрываемых понятий, теорий, явлений, наблюдается умение аргументировано обосновать свою точку зрения, используя терминологию науки, ответ изложен литературным языком в терминах науки. Абитуриент обнаруживает полное и прочное знание содержания программы, демонстрирует глубину понимания существа раскрываемого вопроса. Речь логически обоснованная, правильная с точки зрения грамматики и стилистики.

31 - 40 баллов - дан полный, развернутый ответ на поставленный вопрос, показано умение выделить существенные и несущественные признаки, причинно-следственные связи. Абитуриент испытывает затруднения аргументировано обосновать свою точку зрения, используя терминологию науки. Ответ четко структурирован, логичен, изложен литературным языком в терминах науки. Могут быть допущены недочеты или незначительные ошибки, исправленные с помощью преподавателя. Абитуриент демонстрирует прочное знание программного материала при малозначительных неточностях, пропусках, ошибках.

21-30 баллов - дан недостаточно полный ответ, логика и последовательность изложения имеют нарушения, допущены ошибки в раскрытии понятий, употреблении терминов, отсутствует аргументированность полученных выводов. Абитуриент может конкретизировать обобщенные знания, доказав на примерах их основные положения только с помощью преподавателя. Речевое оформление требует поправок, коррекции. Обнаруживаются грубые ошибки в ответах на уточняющие вопросы преподавателя.

11 - 20 баллов - дан неполный ответ, логика и последовательность изложения имеют существенные нарушения, допущены грубые ошибки при определении сущности раскрываемых понятий. В ответе отсутствуют выводы. Умение раскрыть конкретные проявления обобщенных знаний не показано. Речевое оформление требует поправок, коррекции.

0 - 10 баллов - ответ представляет собой разрозненные знания по теме вопроса с существенными ошибками в определениях. Присутствуют фрагментарность, нелогичность изложения. Отсутствуют выводы, конкретизация и доказательность изложения. Речь неграмотная. Дополнительные и уточняющие вопросы преподавателя не приводят к коррекции ответа абитуриента на поставленный вопрос.

Результаты проведения вступительного экзамена для каждого соискателя оформляются персональным протоколом, в котором фиксируются основные и дополнительные вопросы, а также указываются результаты экзамена в форме оценок по стобалльной шкале. После утверждения протокола проведения вступительного экзамена и его окончательных результатов данный документ хранится в личном деле соискателя.

Решение экзаменационной комиссии размещается на официальном сайте и на информационном стенде приемной комиссии не позднее трех дней с момента проведения вступительного экзамена.

## 3. Содержание программы вступительного экзамена в аспирантуру по специальной дисциплине для направления подготовки 10.06.01 – Информационная безопасность, направленность «Методы и системы защиты информации, информационная безопасность»

### НАУЧНЫЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ.

Понятие национальной безопасности; виды безопасности; информационная безопасность (ИБ) в системе национальной безопасности Российской Федерации. Общеметодологические принципы теории ИБ, анализ угроз ИБ. Проблемы информационного противоборства; государственная политика в информационной сфере; региональные проблемы информационной безопасности. Виды категорий информации; классификация методов и средств обеспечения ИБ. Классификация угроз конфиденциальности, целостности и доступности информации; классификация каналов утечки и искажения информации. Архитектура электронных систем обработки данных; формальные модели. Модели безопасности. Политика безопасности. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем.

Характеристика стандартов по оценке защищенных систем. Построение парольных систем, примеры практической реализации. Особенности применения криптографических методов; способы реализации криптографической подсистемы. Особенности реализации систем с симметричными и несимметричными ключами; концепция защищенного ядра. Классификация методов верификации и исследования корректности систем защиты. Классификация методов построения защищенных автоматизированных систем. Методология обследования и проектирования систем защиты. Особенности управления процессами функционирования систем защиты.

Определение и место проблем информационной безопасности в общей совокупности информационных проблем современного общества. Анализ развития подходов к защите информации. Современная постановка задачи защиты информации. Особенности и состав научно-методологического базиса решения задач защиты информации. Общеметодологические принципы формирования теории защиты информации. Основное содержание теории защиты информации. Модели систем и процессов защиты информации. Определение и содержание понятия угрозы информации в современных системах ее обработки. Системная классификация угроз. Система показателей уязвимости информации. Методы и модели оценки уязвимости информации. Постановка задачи определения требований к защите информации. Методы оценки параметров защищаемой информации. Факторы, влияющие на требуемый уровень защиты информации. Определение и общеметодологические принципы построения систем защиты информации. Основы архитектурного построения систем защиты. Типизация и стандартизация систем защиты. Основные выводы из истории развития теории и практики защиты информации. Перспективы развития теории и практики защиты. Трансформация проблемы защиты информации в проблему обеспечения информационной безопасности.

### ОСНОВЫ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ.

Понятие микропроцессора (МП); обобщенная структура МП; поколения МП и их основные характеристики; перспективные МП. Организация и структура памяти, системы прерывания; системы ввода-вывода; периферийные устройства. Архитектура ПЭВМ, рабочих станций и серверов, системная магистраль, буферизация шин, управление системной магистралью, подключение дополнительных и интерфейсных схем. Универсальные и специализированные ЭВМ высокой производительности; архитектура специализированных вычислительных комплексов, ориентированных на программное обеспечение, машины баз данных, объектно-ориентированная архитектура. Оценка качества программного обеспечения.

Общие принципы методы и средства проектирования архитектуры и структуры, проектирования логики, тестирования и отладки, документирования и сопровождения

программного обеспечения с учетом повышенных требований к надежности программ и их защищенности от несанкционированного доступа. Особенности разработки и сопровождения программного обеспечения для рабочих групп. Internet-технологии, технологии виртуального программирования и объектно-ориентированного программирования. Применение математических методов в проектировании надежного и защищенного программного обеспечения: функциональное программирование, логическое программирование, аналитическое программирование. Структуры данных и абстракции данных; элементарные и простые структуры данных; сложные структуры данных. Оценка сложности алгоритмов; модели вычислений. Алгоритмы сортировки, алгоритмы поиска, Алгоритмы на графах. Генерация случайных последовательностей. Параллельные алгоритмы: методы проектирования параллельных алгоритмов, использование транспьютеров при реализации параллельных алгоритмов, оценки сложности.

Общие принципы построения и использования языков программирования; средства описания данных; средства описания действий. Абстрактные типы данных: инкапсуляция, спецификация, реализация, параметризация, классы и объекты. Обработка файлов; обработка исключительных ситуаций. Параллельная обработка данных. Макропроцессоры и макрогенераторы; современные интегрированные среды разработки программ; отладчики; генераторы кода приложений; библиотеки программ и классов. Стандарты языков программирования, графический интерфейс пользователя. Общая характеристика языков ассемблера: назначение, принципы построения и использования; структура языка, основные группы команд, операторы, средства взаимодействия с операционной системой. Общая характеристика операционных систем. Интерфейс ОС с пользователями; диалоговые и пакетные интерфейсы. Управление ресурсами: управление процессорами; управление памятью; управление устройствами. Драйверы внешних устройств. Классификация, общая характеристика файловых систем. Управление программами: понятие программы, организация динамических и статических вызовов, взаимодействие ОС с программами и отладчиками. Управление процессами: состояния процессов, синхронизация процессов, обмен сообщениями, стратегии и дисциплины планирования, наследование ресурсов, тупиковые ситуации, обработка исключений, сохранение и восстановление процессов.

## ВЫЧИСЛИТЕЛЬНЫЕ СЕТИ

Классификация сетей по способам распределения данных, сравнительная характеристика различных типов сетей; основы организации и функционирования сетей. Сетевые операционные системы; основные сетевые стандарты. Средства взаимодействия процессов в сетях. Распределенная обработка информации в системах клиент-сервер; одноранговые сети.

Безопасность ресурсов сети: средства идентификации и аутентификации, методы разделения ресурсов и технологии разграничения доступа. Средства повышения надежности функционирования сетей. Интеграция локальных сетей в региональные и глобальные сети. Организация вычислительных сетей на базе операционных систем: основные протоколы, службы, функционирование, средства обеспечения безопасности, средства управления и контроля, генерация, сопровождение и разработка приложений; неоднородные вычислительные сети.

Глобальная сеть Internet: основные службы и предоставляемые услуги, основные протоколы, особенности реализации на различных платформах, стандарты. Глобальная сеть Internet: технологии обеспечения безопасности, функционирование, разработка и сопровождение приложений. Современные виды информационного обслуживания; факсимильная передача информации; электронная почта; телеконференция; видеотекс; телетекст; сети связи; структура сетей связи. Методы коммутации информации; особенности сетей с коммутацией каналов, сообщений и пакетов. Эталонная модель взаимодействия открытых систем; общие сведения о протоколах эталонной семиуровневой модели. Глобальные и локальные сети; особенности современных сетевых

архитектур; архитектурные особенности современных локальных сетей; протоколы физического и канального уровней.

## БАЗЫ ДАННЫХ

Общие принципы построения баз данных: реляционная, иерархическая и сетевая модели. Распределенные базы данных в сетях ЭВМ. Общая характеристика, назначение и возможности систем управления базами данных (СУБД). Языковые средства СУБД для различных моделей данных; языковые средства манипулирования данными в реляционных СУБД; языковые средства описания данных реляционных СУБД. Особенности языковых средств управления и обеспечения безопасности данных в реляционных СУБД. Технологии удаленного доступа к системам баз данных, тиражирование и синхронизация в распределенных системах баз данных. Оптимизация производительности и характеристик доступа к базам данных.

## СИСТЕМЫ ПЕРЕДАЧИ ДАННЫХ

Информация, данные, сигналы. Источники информации и ее носители. Количество информации и энтропия. Формулы Хартли и Шеннона. Характеристики процесса передачи информации. Математические модели каналов связи и их классификация. Помехоустойчивость передачи информации. Пропускная способность каналов связи. Теорема Шеннона для каналов без помех и с ними. Типы сигналов, их дискретизация и восстановление. Спектральная плотность сигналов. Частота Найквиста, теорема Котельникова. Частотное представление дискретных сигналов. Ортогональные преобразования дискретных сигналов. Задачи интерполяции и прореживания сигналов. Классификация кодов. Линейные коды. Оптимальное кодирование. Геометрический подход к кодированию. Неравномерные коды Хемминга. Циклические коды. Помехоустойчивое кодирование. Корректирующие коды.

Аналого-цифровые и цифро-аналоговые преобразователи; быстрые преобразования. Цифровые фильтры. Нелинейное и параметрическое преобразование сигналов; модуляция и демодуляция; преобразование частоты.

Классификация систем связи; кодирование информации в системах связи. Методы модуляции в системах связи; основные типы модемов; уплотнение информации в системах связи; дискретные вокодеры. Особенности цифровых систем многоканальных передач сообщений: способы объединения цифровых потоков; особенности передачи дискретных сообщений по цифровым каналам. Системы телефонной связи; цифровая телефония; системы телеграфной связи. Коротковолновые и ультракоротковолновые системы связи; радиорелейные системы связи; телевизионные системы; спутниковые системы связи; волоконно-оптические системы связи. Технические характеристики и принципы функционирования современных модемов. Маршрутизация и управление потоками в сетях связи; сети интегрального обслуживания.

## МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Классификация шифр-систем с секретным ключом. Шифр–системы поточного шифрования (синхронные и асинхронные). Итерационные системы блочного шифрования (шифры Фейстеля, IDEA, RIJNDAEL). Режимы шифрования. Автоматные модели шифров. Системный подход к построению практически стойких шифров. Характеристики случайности и непредсказуемости выходных последовательностей генераторов (периодичность, линейная сложность, статистические характеристики).

Характеристики нелинейности отображений, реализуемых алгоритмами шифрования (сбалансированность, совершенность, строгий лавинный критерий, совершенная нелинейность, корреляционный иммунитет). Генераторы на основе линейных регистров сдвига (фильтрующие, комбинирующие, с неравномерным движением).

Криптография с открытым ключом. Предпосылки появления. Однонаправленные и однонаправленные функции с секретом и их применения. Схемы шифрования с открытым

ключом и цифровой подписи. Основные принципы. Схемы шифрования и подписи RSA и Рабина. Схемы открытого шифрования Эль Гамаля. Сравнение криптосистем с открытым и секретным ключом. Новые схемы шифрования.

Электронная цифровая подпись. Основные понятия. Схемы цифровой подписи RSA и Рабина и их применение. Схема цифровой подписи Эль Гамаля и ее модификации. Способы ускорения процедур подписи и проверки. Стандарты цифровой подписи США (RSA) и России (ГОСТ Р 34.10). Методы генерации секретных параметров для стандартов цифровой подписи. Разновидности схем электронной цифровой подписи и их применение.

## ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ И ФИЗИЧЕСКАЯ ЗАЩИТА

Виды, источники и носители защищаемой информации; демаскирующие признаки объектов наблюдения и сигналов; опасные сигналы и их источники. Побочные электромагнитные излучения и наводки; структура, классификация и основные характеристики технических каналов утечки информации; классификация технической разведки; основные этапы и процедуры добывания информации технической разведкой; возможности видов технической разведки. Методы и средства инженерной защиты и технической охраны объектов; скрытие объектов наблюдения.

Скрытие речевой информации в каналах связи; энергетическое скрытие акустических информативных сигналов; обнаружение и локализация закладных устройств, подавление их сигналов; подавление опасных сигналов акустоэлектрических преобразователей. Экранирование и компенсация информативных полей; подавление информативных сигналов в цепях заземления и электропитания; подавление опасных сигналов. Характеристика государственной системы противодействия технической разведке; нормативные документы по противодействию технической разведке. Основные положения методологии инженерно-технической защиты информации. Виды контроля эффективности защиты информации, методы расчета и инструментального контроля показателей защиты информации. Средства и методы физической защиты объектов; системы сигнализации, видеонаблюдения, контроля доступа. Концепция инженерно-технической защиты информации (ИТЗИ): характеристика ИТЗИ как области информационной безопасности; основные задачи, показатели эффективности и факторы, влияющие на эффективность ИТЗИ; базовые принципы и основные направления ИТЗИ.

Основные методы и средства защиты информации от утечки по техническим каналам. Основные методы и средства инженерной защиты и технической охраны объектов. Основные методы и средства защиты информации в каналах связи. Организация и обеспечение ограничения доступа, пропускного и внутри объектового решения, охрана объектов в процессе транспортировки. Защита информации при авариях, экстремальных ситуациях и в условиях чрезвычайного положения.

## ПРОГРАММНО-АППАРАТНЫЕ МЕТОДЫ ЗАЩИТЫ ОТ НСД

Основные принципы создания программно-аппаратных средств обеспечения информационной безопасности, концепция диспетчера доступа. Методы и средства ограничения доступа к компонентам вычислительных систем; методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям; методы и средства хранения ключевой информации. Защита программ от изучения, способы встраивания средств защиты в программное обеспечение. Защита от разрушающих программных воздействий, защита программ от изменения и контроль целостности, построение изолированной программной среды.

Программно-аппаратные средства защиты информации в сетях передачи данных. Организация управления доступом и защиты ресурсов ОС; основные механизмы безопасности: средства и методы аутентификации в ОС. Модели разграничения доступа, организация и использование средств аудита. Администрирование ОС: задачи и принципы сопровождения системного программного обеспечения, генерация, настройка, измерение производительности и модификация систем, управление безопасностью ОС; основные

стандарты ОС. Перспективы развития; основные механизмы обеспечения безопасности и управления распределенными ресурсами. Основные положения критериев TB CSEC («Оранжевая книга»). Фундаментальные требования компьютерной безопасности. Требования классов защищенности.

Основные положения Руководящих документов Гостехкомиссии России в области за-щиты информации. Определение и классификация нарушителя. Классы защищенности АС от НСД к информации. Основные положения CITCE («Единые критерии»). Структура профиля и проекта защиты. Структура и ранжирование функциональных требований. Требования доверия. Языковые средства представления информации в Internet Организация защиты корпоративных сетей Internet. Средства обеспечения безопасности баз данных: средства идентификации и аутентификации объектов баз данных, языковые средства разграничения доступа, концепция и реализация механизма ролей. Организация аудита событий в системах баз данных; средства контроля целостности информации, организация взаимодействия СУБД и базовой ОС, журнализация, средства создания резервных копии и восстановления баз данных. Задачи и средства администратора безопасности баз данных. Средства реализации диалогового интерфейса и подготовки отчетов в языках СУБД. Средства автоматизации проектирования баз данных.

## ОРГАНИЗАЦИОННО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ

Анализ и оценка угроз информационной безопасности объекта управления. Методология оценки ущерба от злоумышленных и неумышленных противоправных нарушений безопасности информации. Цели и задачи службы безопасности объекта информации. Организационная структура. Особенности функционирования структурных подразделений. Организация и обеспечение ограничения доступа, пропускного и внутри объектового решения, охрана объектов в процессе транспортировки, защита информации при авариях, экстремальных ситуациях и в условиях чрезвычайного положения.

Понятие секретного (конфиденциального) делопроизводства. Общие принципы его организации. Механизм и процедуры установления степени секретности (конфиденциальности). Правила оформления документов с ограниченным доступом. Правила и формы регистрации документов. Размножение, правила приема и передачи. Обеспечение сохранности документов с ограниченным доступом. Организация хранения. Требования к помещениям и хранилищам. Правила и порядок уничтожения документов с ограниченным доступом. Контроль и методы проверки состояния делопроизводства с ограниченным доступом. Порядок проведения служебных расследований случаев нарушения порядка специального делопроизводства. Особенности организации электронного документооборота. Система удостоверения ЭЦП. Цели, задачи и особенности функционирования удостоверяющих центров. Особенности организации системы мониторинга и сетевого аудита. Взаимодействие с правоохранительными органами.

Методы и средства подбора и расстановки кадров. Особенности взаимодействия служб безопасности с персоналом предприятия. Система обеспечения психологической устойчивости к криминальным воздействиям. Методы психофизиологического тестирования. Обеспечение безопасности при осуществлении научно-технического, экономического и международного сотрудничества. Служба безопасности объекта; подбор, расстановка и работа с кадрами; организация и обеспечение режима секретности; организация пропускного и внутриобъектового режима; организация режима и охраны объектов в процессе транспортировки. Защита информации при авариях, иных экстремальных ситуациях и в условиях чрезвычайного положения; технологические меры поддержания информационной безопасности объектов.

Законодательство РФ в области информационной безопасности, защиты государственной тайны и конфиденциальной информации; конституционные гарантии прав граждан на информацию и механизм их реализации. Понятие и виды защищаемой информации по законодательству РФ; государственная тайна как особый вид защищаемой информации; конфиденциальная информация. Система защиты государственной тайны;

правовой режим защиты государственной тайны; правовое регулирование взаимоотношений администрации и персонала в области защиты информации; правовые режимы конфиденциальной информации.

Лицензирование и сертификация в области защиты информации, в том числе государственной тайны. Задачи и технология сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности; основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности. Правовые основы защиты информации с использованием технических средств (защита от технических разведок, применение шифровальных средств, электронная цифровая подпись и т.д.). Защита интеллектуальной собственности. Правовая регламентация охранной деятельности. Международное законодательство в области защиты информации. Преступления в сфере компьютерной информации; экспертиза преступлений в области компьютерной информации; криминалистические аспекты проведения расследований.

## ПРОЕКТИРОВАНИЕ ЗАЩИЩЕННЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Постановка проблемы комплексного обеспечения информационной безопасности автоматизированных систем; состав компонентов комплексной системы обеспечения информационной безопасности (КСИБ), функциональные и обеспечивающие подсистемы, технология, управление. Методология формирования задач защиты; интеграция средств информационной безопасности в технологическую среду; этапы проектирования КСИБ и требования к ним: предпроектное обследование, техническое задание, техническое проектирование, рабочее проектирование, испытания и внедрение в эксплуатацию, сопровождение. Особенности проектирования на современном уровне и синтез КСИБ; типовая структура комплексной системы защиты информации от несанкционированного доступа (НСД).

Методы и методики проектирования: методика выявления возможных каналов НСД, последовательность работ при проектировании комплексной системы защиты информации от НСД и утечки за счет ПЭМИН, моделирование как инструментарий проектирования. Методы и методики оценки качества КСИБ: методы нормативного функционального наполнения, метод экспертных структурных вопросников, метод оценки уязвимости информации Хоффмана, метод оценки риска Фишера.

Аттестация автоматизированных систем по требованиям безопасности информации. Особенности эксплуатации КСИБ на объекте защиты, организационно-функциональные задачи службы безопасности, управление информационной безопасностью объекта. Безопасность и экологичность технических систем; безопасность в чрезвычайных ситуациях. Управление безопасностью жизнедеятельности. Основы электробезопасности; безопасность систем связи. Анатомо-физиологические и психологические воздействия на человека опасных и вредных факторов при работе с защищенными автоматизированными системами. Понятие сложной системы: элементы и подсистемы, управление и информация, самоорганизация; основные принципы системного подхода при создании сложных систем. Понятие качества и эффективности: характеристики качества, показатели и критерии эффективности, методические вопросы оценки эффективности сложных систем. Функциональная и обеспечивающая часть сложной системы; технология функционирования сложной системы; цели и задачи проектирования; структуризация предметной области; классификация объектов проектирования.

Жизненный цикл автоматизированной системы; этапы проектирования системы; организация работ, функции заказчиков и разработчиков. Практические методы реализации моделей безопасности; ядра безопасности; мониторинг взаимодействий в системе; архитектура защищенных систем. Принципы построения защищенных информационных систем; технологический цикл реализации защищенной системы обработки и хранения информации. Реализация систем контроля доступа; способы представления информации о правах доступа.

## 4. Вопросы к вступительному экзамену в аспирантуру по специальной дисциплине для направления подготовки 10.06.01 – информационная безопасность, направленность «Методы и системы защиты информации, информационная безопасность»

1. Сущность и этапы системного подхода к исследованию проблем информационной безопасности.
2. Система защиты информации как объект исследования.
3. Основные понятия и определения математической статистики. Статистическая проверка гипотез.
4. Случайные процессы. Марковские процессы.
5. Назначение и классификация математических моделей. Этапы моделирования сложных процессов.
6. Структурное и объектно-ориентированное описание информационных процессов и систем на основе инструментальных средств CASE-технологий.
7. Сущность и вычислительная схема метода статистических испытаний.
8. Элементы теории массового обслуживания. Потоки событий и их характеристики. Многоканальные системы массового обслуживания.
9. Элементы теории систем. Принципы системного анализа.
10. Концептуальная модель информационной системы.
11. Назначение, классификация и компонентный состав информационных систем.
12. База данных. Основные модели баз данных.
13. Общие требования к защите информации в автоматизированных системах.
14. Методология (этапы) проектирования автоматизированных систем.
15. Методы расчёта и оценки характеристик автоматизированных систем.
16. Основные положения концепции информационной безопасности России.
17. Классификация и характеристика основных угроз предпринимательской деятельности.
18. Структура системы безопасности предпринимательской деятельности. Информационно-коммерческая защита.
19. Гарантии информационной безопасности. Международные стандарты.
20. Коммерческая информация в бизнесе. Проблемы защиты коммерческой информации.
21. Проблемы защиты коммерческой информации в организациях различных форм собственности.
22. Каналы утечки коммерческой информации.
23. Структура комплексных систем защиты информации в автоматизированных системах, использующих сочетание различных методов и средств.
24. Технические и эксплуатационные характеристики систем защиты информации, хранимой и обрабатываемой в автоматизированных системах.
25. Требования к архитектуре и инструментальным средствам системы защиты информации.
26. Методы организации и руководства обеспечением системы информационной безопасности в сфере защиты промышленных и коммерческих секретов.
27. Классификация и характеристика методов защиты информации в автоматизированных системах.
28. Методы и модели для оценки эффективности систем защиты информации в условиях противодействия.
29. Тенденции в области создания аппаратных и программных средств системы защиты информации в автоматизированных системах.
30. Программные средства защиты информации в автоматизированных системах.
31. Физические методы и средства защиты информации в автоматизированных системах.
32. Организационные методы и средства защиты информации в

автоматизированных системах.

33. Криптографические методы защиты информации в автоматизированных системах.

34. Информационные угрозы. Их оценка и прогнозирование.

35. Информационные технологии в структуре системы управления безопасностью предпринимательства.

36. Принципы построения вычислительных систем и сетей.

37. Модели задач синтеза базовых компонентов системы защиты информации в локальных вычислительных сетях.

38. Нормативные акты и стандарты по проблеме информационной безопасности.

39. Принципы и нормы правового обеспечения информационной безопасности населения и предприятий различных форм собственности.

40. Принципы законодательного, нормативного и правового регулирования вопросов информационной безопасности.

41. Тенденции в области создания информационного и программного обеспечения вычислительных сетей.

42. Методы дискретной оптимизации в задачах проектирования информационных систем.

43. Инструментальные и программные средства поддержки задач проектирования информационных систем.

44. Принципы модульности, типизации и унификации при построении информационных систем. Факторы окружающей среды и их влияние на эффективность автоматизированных систем.

45. Принципы классической криптографии. Системы блочного шифрования: DES и ГОСТ.

46. Компьютерные вирусы, их классификация. Средства антивирусной защиты. Вирусное подавление как форма информационной войны.

47. Защита информации от утечки по техническим каналам. Основные виды технических каналов и источников утечки информации. Методы предотвращения утечки информации.

48. Концепция комплексной защиты информации. Методология создания, организации и обеспечения функционирования систем комплексной защиты информации.

49. Особенности правовой поддержки информационной безопасности на различных стадиях жизненного цикла автоматизированной системы.

50. Инструментальные и программные средства поддержки задач проектирования; графические средства представления проектных решений.

## 5. Литература

## 4. Вопросы к вступительному экзамену в аспирантуру по специальной дисциплине для направления подготовки 10.06.01 – информационная безопасность, направленность «Методы и системы защиты информации, информационная безопасность»

1. Сущность и этапы системного подхода к исследованию проблем информационной безопасности.

2. Система защиты информации как объект исследования.

3. Основные понятия и определения математической статистики. Статистическая проверка гипотез.

4. Случайные процессы. Марковские процессы.

5. Назначение и классификация математических моделей. Этапы моделирования сложных процессов.

6. Структурное и объектно-ориентированное описание информационных процессов и систем на основе инструментальных средств CASE-технологий.

7. Сущность и вычислительная схема метода статистических испытаний.

8. Элементы теории массового обслуживания. Потоки событий и их

характеристики. Многоканальные системы массового обслуживания.

9. Элементы теории систем. Принципы системного анализа.
10. Концептуальная модель информационной системы.
11. Назначение, классификация и компонентный состав информационных систем.
12. База данных. Основные модели баз данных.
13. Общие требования к защите информации в автоматизированных системах.
14. Методология (этапы) проектирования автоматизированных систем.
15. Методы расчёта и оценки характеристик автоматизированных систем.
16. Основные положения концепции информационной безопасности России.
17. Классификация и характеристика основных угроз предпринимательской деятельности.
18. Структура системы безопасности предпринимательской деятельности. Информационно-коммерческая защита.
19. Гарантии информационной безопасности. Международные стандарты.
20. Коммерческая информация в бизнесе. Проблемы защиты коммерческой информации.
21. Проблемы защиты коммерческой информации в организациях различных форм собственности.
22. Каналы утечки коммерческой информации.
23. Структура комплексных систем защиты информации в автоматизированных системах, использующих сочетание различных методов и средств.
24. Технические и эксплуатационные характеристики систем защиты информации, хранимой и обрабатываемой в автоматизированных системах.
25. Требования к архитектуре и инструментальным средствам системы защиты информации.
26. Методы организации и руководства обеспечением системы информационной безопасности в сфере защиты промышленных и коммерческих секретов.
27. Классификация и характеристика методов защиты информации в автоматизированных системах.
28. Методы и модели для оценки эффективности систем защиты информации в условиях противодействия.
29. Тенденции в области создания аппаратных и программных средств системы защиты информации в автоматизированных системах.
30. Программные средства защиты информации в автоматизированных системах.
31. Физические методы и средства защиты информации в автоматизированных системах.
32. Организационные методы и средства защиты информации в автоматизированных системах.
33. Криптографические методы защиты информации в автоматизированных системах.
34. Информационные угрозы. Их оценка и прогнозирование.
35. Информационные технологии в структуре системы управления безопасностью предпринимательства.
36. Принципы построения вычислительных систем и сетей.
37. Модели задач синтеза базовых компонентов системы защиты информации в локальных вычислительных сетях.
38. Нормативные акты и стандарты по проблеме информационной безопасности.
39. Принципы и нормы правового обеспечения информационной безопасности населения и предприятий различных форм собственности.
40. Принципы законодательного, нормативного и правового регулирования вопросов информационной безопасности.
41. Тенденции в области создания информационного и программного обеспечения вычислительных сетей.
42. Методы дискретной оптимизации в задачах проектирования информационных

систем.

43. Инструментальные и программные средства поддержки задач проектирования информационных систем.

44. Принципы модульности, типизации и унификации при построении информационных систем. Факторы окружающей среды и их влияние на эффективность автоматизированных систем.

45. Принципы классической криптографии. Системы блочного шифрования: DES и ГОСТ.

46. Компьютерные вирусы, их классификация. Средства антивирусной защиты. Вирусное подавление как форма информационной войны.

47. Защита информации от утечки по техническим каналам. Основные виды технических каналов и источников утечки информации. Методы предотвращения утечки информации.

48. Концепция комплексной защиты информации. Методология создания, организации и обеспечения функционирования систем комплексной защиты информации.

49. Особенности правовой поддержки информационной безопасности на различных стадиях жизненного цикла автоматизированной системы.

50. Инструментальные и программные средства поддержки задач проектирования; графические средства представления проектных решений.

## 5. Литература

**а) основная литература:**

1. Загинайлов, Ю. Н. Теория информационной безопасности и методология защиты информации / Ю.Н. Загинайлов. - М.; Берлин: Директ-Медиа, 2015. - 253 с.: ил. - Библиогр. в кн. - ISBN 978-5-4475-3946-7; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=276557

2. Методологические основы построения защищенных автоматизированных систем: учебное пособие / А.В. Душкин, О.В. Ланкин, С.В. Потехецкий и др.; Министерство образования и науки РФ, ФГБОУ ВПО «Воронежский государственный университет инженерных технологий». - Воронеж: Воронежская государственная лесотехническая академия, 2013. - 258 с.: табл., ил. - Библиогр. в кн. - ISBN 978-5-89448-981-0; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=255851

3. Петров, С. В. Информационная безопасность : учебное пособие для студентов вузов / С. В. Петров, П. А. Кисляков ; Министерство образования и науки РФ; ФЦП "Научные и научно-педагогические кадры инновационной России" на 2009-2013 годы. - Москва: Русский журнал, 2011. - 328 с.

**б) дополнительная литература:**

1. Арутюнов, В. В. Защита информации : учебно-методическое пособие / В. В. Арутюнов. - Москва: Либерея-Бибинформ, 2008. - 56 с.

2. Гайдамакин, Н. А. Автоматизированные информационные системы, базы и банки данных: вводный курс: учебное пособие / Н. А. Гайдамакин. - Москва: Гелиос АРВ, 2002. - 368 с.

3. Галатенко, В.А. Основы информационной безопасности: курс лекций: учебное пособие / В. А. Галатенко; Интернет университет информационных технологий; под ред. В. Б. Бетелина. - 2-е изд.; испр. - Москва: Интернет-Университет Информационных Технологий, 2004. - 264 с.

4. Гашков, С. Б. Криптографические методы защиты информации: учебное пособие для студентов вузов / С. Б. Гашков, Э. А. Применко, М. А. Черепнев. - Москва: Академия, 2010. - 304 с.

5. Дейт, К. Дж. Введение в системы баз данных: пер. с англ. / Дейт, К. Дж. - 8-е изд. - Санкт-Петербург: Вильямс, 2008. - 1328 с.

6. Диго, С. М. Базы данных: проектирование и использование: учебник для студентов вузов / С. М. Диго. - Москва: Финансы и статистика, 2005. - 592 с.

7. Ибрагимов, И. М. Информационные технологии и средства дистанционного обучения: учебное пособие для студентов высших учебных заведений / И. М. Ибрагимов ; под ред. А. Н. Ковшова. - 3-е изд. ; стер. - Москва: Академия, 2008. - 336 с.

8. Кузин, А. В. Базы данных: учебное пособие для студентов вузов / А. В. Кузин, С. В. Левонисова. - 4-е изд. ; стер. - Москва: Академия, 2010. - 320 с.

9. Мартишин, С. А. Проектирование и реализация баз данных в СУБД MySQL с использованием MySQL Workbench: учебное пособие / С. А. Мартишин, В. Л. Симонов, М. В. Храпченко. - Москва: Форум: Инфра-М, 2012. - 160 с.

10. Мельников, В. П. Информационные технологии: учебник / В. П. Мельников. - Москва: Академия, 2008. - 432 с.

11. Одинцов, А. А. Экономическая и информационная безопасность: справочник: учебное пособие для вузов / А.А. Одинцов. - Москва: Экзамен, 2005. - 576 с.

12. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы : учебное пособие / В. Г. Олифер, Н. А. Олифер. - 3-е изд. - Санкт-Петербург : Питер, 2006. - 960 с. : ил.

13. Олифер, В. Г. Основы сетей передачи данных : курс лекций : учебное пособие / В. Г. Олифер, Н. А. Олифер ; Интернет университет информационных технологий. - 2-е изд. ; испр. - Москва: Интернет-Университет Информационных Технологий, 2005. - 176 с.

14. Попов, В. Б. Основы информационных и телекоммуникационных технологий. Основы информационной безопасности: учебное пособие / В.Б. Попов. - Москва: Финансы и статистика, 2005. - 176 с.

15. Расторгуев, С.П. Основы информационной безопасности: учебное пособие для студентов высших учебных заведений / С.П. Расторгуев. - Москва: Академия, 2007. - 192с.

16. Рудинский, И. Д. Технология проектирования автоматизированных систем обработки информации и управления: учебное пособие для студентов вузов / И. Д. Рудинский. - Москва: Горячая линия-Телеком, 2011. - 304 с.

17. Сергеева, Ю.С. Защита информации: Конспект лекций : учебное пособие / Ю.С. Сергеева. - М.: А-Приор, 2011. - 128 с. - (Конспект лекций). - ISBN 978-5-384-00397-7; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=72670

18. СУБД: язык SQL в примерах и задачах: учебное пособие для студентов высших учебных заведений / И. Ф. Астахова [и др.]. - Москва: Физматлит, 2009. - 168 с.

19. Сычев, Ю.Н. Основы информационной безопасности: учебно-практическое пособие / Ю.Н. Сычев. - М.: Евразийский открытый институт, 2010. - 328 с. - ISBN 978-5-374-00381-9; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=90790

20. Фаронов, А.Е. Основы информационной безопасности при работе на компьютере / А.Е. Фаронов. - М.: Интернет-Университет Информационных Технологий, 2011. - 138 с.; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=233763

21. Хаулет, Т. Защитные средства с открытыми исходными текстами: Практическое руководство по защитным приложениям : учебное пособие / Т. Хаулет ; Национальный Открытый Университет "ИНТУИТ" ; пер. с англ. В. Галатенко, О. Труфанов ; под ред. В. Галатенко. - М. : Интернет-Университет Информационных Технологий, 2007. - 608 с. : ил., табл., схем. - (Основы информационных технологий). - ISBN 978-5-94774-629-7; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=233306

22. Ярочкин, В.И. Информационная безопасность / В.И. Ярочкин. - Москва: Академический Проект: Гаудеамус, 2004. - 544 с.

**в) программное обеспечение и Интернет-ресурсы:**

1. Информационно-аналитический портал socpolitika.ru. Режим доступа: http://www.socpolitika.ru/rus/social_policy_monitoring/comments/document5869.shtml
2. Научно-методический журнал "Информатизация образования и науки" // http://www.informika.ru/about/informatization_pub/about/276/
3. Сайт ФГУ ГНИИ ИТТ "Информика" - www.informika.ru
4. Студенческое интернет сообщество – www.students.ru

5. Электронная библиотечная система http://www.book.ru
6. Библиотека программиста http://www.coders-library.ru

Список литературы согласован
«26» июня 2018 г. _____ Н.А. Алексеева



Программа одобрена на заседании кафедры информационных систем и технологий Шуйского филиала ФГБОУ ВО «Ивановский государственный университет» «27» июня 2018 года, протокол № 11.