**«ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»
(Финансовый университет)**

Департамент информационной безопасности

Факультет информационных технологий и анализа больших данных

УТВЕРЖДАЮ

Проректор по учебной
и методической работе

_____Е.А. Каменева
«___» _____ 2022 г.

Козьминых С.И.

«МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

подготовки научно-педагогических кадров в аспирантуре

по научной специальности «2.3.6 - Методы и системы защиты информации, информационная безопасность»

ПРОГРАММА КАНДИДАТСКОГО ЭКЗАМЕНА

Одобрено учебно-научным Департаментом информационной безопасности (протокол № 12 от «14» ноября 2022 г.)

Москва 2022

СОДЕРЖАНИЕ

Раздел 1. Требования к результатам освоения программы и результатам обучения по дисциплине, выносимой на кандидатский экзамен

Наименование дисциплины

Методы и системы защиты информации, информационная безопасность

Код компетенции	Наименование компетенции	Индикаторы достижения компетенции	Результаты обучения умения и знания, соотнесенные с компетенциями/индикаторами достижения компетенции
ПКС-1	Способность формулировать научные задачи в области обеспечения информационной безопасности, применять для их решения методологии теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность.	1. Формулирует научные задачи в области обеспечения информационной безопасности. 2. Выявляет и анализирует научные проблемы в области обеспечения информационной безопасности. 3. Применяет методологию теоретических и экспериментальных научных исследований, внедряет полученные результаты в практическую деятельность.	**Знать** как формулировать научные задачи в области обеспечения информационной безопасности **Уметь** формулировать научные задачи в области обеспечения информационной безопасности **Знать** как выявлять и анализировать научные проблемы в области обеспечения информационной безопасности. **Уметь** выявлять и анализировать научные проблемы в области обеспечения информационной безопасности. **Знать** как применять методологию теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность. **Уметь** применять методологию теоретических и эксперимен-

			тальных научных исследований, внедрять полученные результаты в практическую деятельность.
ПКС-2	Способность разрабатывать частные методы исследования и применять их в самостоятельной научно-исследовательской деятельности для решения конкретных исследовательских задач в области обеспечения информационной безопасности.	1. Разрабатывает частные методы исследования и применяет их в самостоятельной научно-исследовательской деятельности для решения конкретных исследовательских задач в области обеспечения информационной безопасности. 2. Работает со значительным массивом информации, оценивая её полноту и достоверность, восполняя и синтезируя недостающую информацию. 3. Разрабатывает инновационные методики и методы исследования для их последующего применения области обеспечения информационной безопасности.	**Знать** как разрабатывать частные методы исследования и применять их в самостоятельной научно-исследовательской деятельности для решения конкретных исследовательских задач в области обеспечения информационной безопасности. **Уметь** разрабатывать частные методы исследования и применять их в самостоятельной научно-исследовательской деятельности для решения конкретных исследовательских задач в области обеспечения информационной безопасности. **Знать** как работать со значительным массивом информации, оценивать её полноту и достоверность, восполняя и синтезируя недостающую информацию. **Уметь** работать со значительным массивом информации, оценивать её полноту и достоверность, восполняя и синтезируя недостающую информацию. **Знать** как разрабатывать инновационные методики и методы исследования для их по-

			следующего применения области обеспечения информационной безопасности. **Уметь** разрабатывать инновационные методики и методы исследования для их последующего применения области обеспечения информационной безопасности.
ПКС-3	Способность обоснованно оценивать степень соответствия защищаемых объектов информатизации и информационных систем действующим стандартам в области информационной безопасности.	1. Проводит обоснованную оценку степени соответствия защищаемых объектов информатизации и информационных систем действующим стандартам в области информационной безопасности. 2. Определяет уровень защищенности объектов информатизации и информационных систем. 3. Демонстрирует применение методологии и методов оценки степени защищенности объектов информатизации и информационных систем.	**Знать** как проводить обоснованную оценку степени соответствия защищаемых объектов информатизации и информационных систем действующим стандартам в области информационной безопасности. **Уметь** проводить обоснованную оценку степени соответствия защищаемых объектов информатизации и информационных систем действующим стандартам в области информационной безопасности. **Знать** как определять уровень защищенности объектов информатизации и информационных систем. **Уметь** определять уровень защищенности объектов информатизации и информационных систем. **Знать** как демонстрировать применение методологии и методов оценки степени защищенности объектов информатизации и ин-

			формационных систем. **Уметь** демонстрировать применение методологии и методов оценки степени защищенности объектов информатизации и информационных систем.
ПКС-4	Способность организовать работу коллектива по проведению научных исследований в области информационной безопасности.	1. Организует работу по проведению научных исследований в области информационной безопасности. 2. Контролирует ход работы по проведению научных исследований в области информационной безопасности. 3. Оценивает результаты работы по проведению научных исследований в области информационной безопасности.	**Знать** как организовать работу по проведению научных исследований в области информационной безопасности. **Уметь** организовать работу по проведению научных исследований в области информационной безопасности. **Знать** как контролировать ход работы по проведению научных исследований в области информационной безопасности. **Уметь** контролировать ход работы по проведению научных исследований в области информационной безопасности. **Знать** как оценивать результаты работы по проведению научных исследований в области информационной безопасности. **Уметь** оценивать результаты работы по проведению научных исследований в области информационной безопасности.
ПКС-5	Готовность к преподавательской деятельности по основным обра-	1. Осуществляет преподавательскую деятельности по основным образовательным	**Знать** как осуществлять преподавательскую деятельности по

	зовательным программам высшего образования.	программам высшего образования в области обеспечения информационной безопасности. 2. Повышает квалификацию по основным образовательным программам высшего образования в области обеспечения информационной безопасности. 3. Разрабатывает новые дисциплины по основным образовательным программам высшего образования в области обеспечения информационной безопасности.	основным образовательным программам высшего образования в области обеспечения информационной безопасности. **Уметь** осуществлять преподавательскую деятельности по основным образовательным программам высшего образования в области обеспечения информационной безопасности. **Знать** как повышать квалификацию по основным образовательным программам высшего образования в области обеспечения информационной безопасности. **Уметь** повышать квалификацию по основным образовательным программам высшего образования в области обеспечения информационной безопасности. **Знать** как разрабатывать новые дисциплины по основным образовательным программам высшего образования в области обеспечения информационной безопасности. **Уметь** разрабатывать новые дисциплины по основным образовательным программам высшего образования в области обеспечения информационной безопасности.

2. Содержание программы кандидатского экзамена

Тема 1. Нормативно-правовые, общие и методологические аспекты защиты информации

Объекты правового регулирования. Основные задачи обеспечения информационной безопасности в информационных системах. Объекты правового регулирования при создании и эксплуатации системы обеспечения информационной безопасности. Использование существующих нормативных актов для создания системы обеспечения информационной безопасности. Основные положения руководящих правовых документов. Обеспечение безопасности государственных и коммерческих информационных ресурсов. Базовые проблемы защиты информации в информационных системах. Определение и классификация компьютерных атак и особенности их обнаружения. Модель угроз безопасности информации в информационных системах. Меры по обеспечению безопасности информации. Нормативно правовое обеспечение информационной безопасности информационных систем. Нормативно-правовое обеспечение информационной безопасности информационных систем. Обзор Российского законодательства в сфере защиты информации в информационных системах. Аспекты защиты коммерческой тайны, предотвращение промышленного шпионажа. Сведения, составляющие банковскую и коммерческую тайну.

Обеспечение безопасности банковской и коммерческой тайны. Аспекты защиты авторского права. Правовая база в сфере защиты банковской тайны. Система международных и российских правовых стандартов. Стандарт ISO 27001:2005. Требования доктрины информационной безопасности РФ и ее реализация в существующих системах информационной безопасности. Практическое составление основных правовых документов (концепции информационной безопасности, плана мероприятий информационной безопасности, инструкции информационной безопасности для рабочего места). Понятие и основные организационные мероприятия по обеспечению информационной безопасности.

Принципы и основы построения систем защиты информации (СЗИ) в информационных системах. Нормативная, методическая и научная базы системы защиты информации (СЗИ) в информационных системах. Инструментальный базис обеспечения информационной безопасности информационных систем. Основополагающие принципы разработки и построения систем обеспечения информационной безопасности информационных систем.

Нормативно-правовая документация по обеспечению информационной безопасности информационных систем: основные требования, содержание, структура и обоснование. Структура, цели и задачи регуляторов (органов), выполняющих и обеспечивающих информационную безопасность информационных систем. Политика информационной безопасности как основа организационных мероприятий. Основные требования в разработке организационных мероприятий. Контроль и моделирование как основные формы организационных действий при проверке действенности системы информационной безопасности. Разграничение прав доступа как основополагающее требование организационных мероприятий и их практическая реализация на объекте защиты. Иерархия прав и обязанностей руководителей и исполнителей при построении системы информационной безопасности, их взаимодействие.

Организационный и правовой статусы службы информационной безопасности информационной системы. Организационные, технические и режимные меры обеспечения информационной безопасности информационных систем. Разграничение прав доступа к защищаемой информации в информационной системе. Разработка и обоснование политики безопасности. Аспекты организации защищённого делопроизводства и мероприятий по защите информационной безопасности информационных систем. Аудит системы информационной безопасности на объекте защиты как основание для подготовки организационных и правовых мероприятий. Его критерии, формы и методы. Правовое обеспечение защиты персональных данных в РФ. Хронология принятия, основные положения нормативных актов и руководящих документов. Система

управления информационной безопасностью (СУИБ). Процессный подход к построению СУИБ и циклическая модель PDCA. Цели и задачи, решаемые СУИБ. Стандартизация в области построения СУИБ: сходства и различия стандартов. Анализ рисков ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ. Основные подходы, основные этапы процесса. Управление непрерывностью деятельности: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ. Единые критерии (ГОСТ Р ИСО 15408).

Профиль защиты. Задание по безопасности. Расследование инцидентов ИБ: виды расследования инцидентов, критерии выбора необходимого вида расследования, основные этапы расследования (для различных видов расследования). Разведка и сбор информации для предотвращения нарушения конфиденциальности, целостности и доступности информации (сканирование сети, поиск и эксплуатация уязвимостей).

Тема 2. Технические средства защиты информации.

Теория информации. Математическая теория связи. Определение информации и энтропии. Сжатие данных. Обнаружение и коррекция ошибок при передаче данных. Определение сигнала, параметры сигнала. Классификация сигналов: непрерывные, дискретные, квантованные по уровню, цифровые сигналы. Кодирование и декодирование информации. Эффективное кодирование информации. Кодирование как средство обеспечения целостности информации. Примеры алгоритмов кодирования. Программно-аппаратная база обеспечения информационной безопасности информационных систем и средства ограничения доступа к компонентам информационной системы.

Технические каналы утечки информации. Классификация демаскирующих признаков и их характеристики. Технические каналы утечки информации, классификация и характеристика. Акустический канал утечки информации. Основные функции и принципы действия технических средств акустической (речевой) разведки. Средства защиты от утечки по акустическому каналу. Виброакустический канал утечки информации. Построение системы защиты информации от утечки по виброакустическому

каналу. Радиоэлектронный канал утечки информации. Общая характеристика и особенности радиоэлектронной разведки. Сканирование и перехват информации с радиотелефонов, офисной техники, кабелей, проходящих через помещение. Электромагнитный канал утечки информации. Низкочастотные и высокочастотные устройства съёма информации. Системы защиты информации от утечки по электромагнитному каналу. Оптический канал утечки информации. Телевизионные системы наблюдения. Материально-вещественный канал утечки информации. Основные методы противодействия утечке информации по материально-вещественному каналу. Классификация видов несанкционированного доступа и основные условия функционирования средств защиты информации. Средства противодействия локальному несанкционированному доступу к информации в информационной системе. Системы контроля доступа. Задачи и требования к техническим средствам защиты информации для обеспечения конфиденциальности информации. Системный анализ базовых проблем инженерно-технической защиты информации в информационных системах. Классификация способов и средств организационных и технических мер защиты информации в информационных системах. Условия и принципы утечки информации. Структура канала утечки информации. Классификация каналов утечки информации. Побочные электромагнитные излучения и наводки как канал утечки информации. Активная и пассивная защита информации. Технический контроль и оценка эффективности мер защиты информации. Назначения, средства, содержание и методы технического контроля. Основные проблемы и направления развития исследований в области технической защиты информации в информационных системах.

Задачи и принципы инженерно-технической защиты информации. Принцип работы телефона и микрофона. Построение системы защиты от негласной записи информации на диктофон. Демаскирующие признаки. Непосредственное прослушивание звуковой информации и прослушивание информации направленными микрофонами. Лазерные системы съема информации, электронные стетоскопы и гидроакустические преобразователи. Определение радиозакладок. Основные характеристики и основные

элементы радиозакладок. Прослушивание информации с помощью внедрённых радиозакладок. Прослушивание информации с помощью пассивных закладок. Приёмники информации с радиозакладок. Технические методы и средства поиска работающих радиозакладок. Применение нелинейных радиолокаторов для поиска радиозакладок. Телефонная линия как один из основных каналов утечки информации. Контактный и бесконтактный способы съема информации с помощью телефонных линий: непосредственное подключение, считывание с помощью трансформаторов, преобразователей Холла, индуктивных датчиков. Принцип действия телефонного аппарата, беззаходовый несанкционированный съем информации, несанкционированное использование микрофона телефонного аппарата, телефонные ретрансляторы. Защита от несанкционированного съёма информации в радиоэлектронных каналах. Устройства уничтожения закладных устройств. Устройства предотвращения утечки информации по телефонному каналу. Предотвращение утечки информации по сотовым сетям связи. Построение, анализ и оценка структурных, функциональных, информационных и комплексных моделей каналов утечки информации. Построение, анализ и оценка моделей систем защиты. Оценка эффективности модели защиты, выбор оптимальной системы защиты информации и выбор соответствующих технических средств защиты информации. Защита программного обеспечения от разрушающих программных воздействий (программных закладок, вирусов) и от реверсивного инжиниринга. Описание взаимодействия прикладной программы и программной закладки. Методы внедрения программных закладных устройств.

Модель изолированной программной среды. Методы верификации защитных механизмов от закладных устройств. Методы защиты от несанкционированного доступа и разрушающих программных воздействий в процессе хранения информации. Основные методы защиты информации техническими средствами.

Тема 3. Основы информационной безопасности.

Основные понятия защиты информации. Основные понятия защиты информации

(субъекты, объекты, доступ, граф доступов, информационные потоки). Постановка задачи построения защищенной автоматизированной системы (АС). Ценность и значимость информации. Угрозы безопасности информации. Угрозы конфиденциальности, целостности доступности АС. Понятие политики безопасности. Дискреционная политика безопасности. Мандатная политика безопасности. Мандатная политика целостности. Модели угроз, и их виды, объекты исследований (антропогенные, техногенные, стихийны источники угроз). Системы обнаружения вторжений (IDS) и системы предотвращения вторжений (IPS). Системы предотвращения утечки информации (DLP): структура системы, цели и задачи, ошибки первого и второго рода. SQL- «инъекции»: основные понятия, цели и задачи «инъекции», пример. Фаззинг как средство нахождения уязвимостей и средство преодоления системы защиты. Атака типа «отказ в обслуживании»: DoS, DDoS. Принцип построения «зомби»- сетей, основные цели атаки. Доступность как одно из ключевых свойств информации. Межсайтовый скриптинг (XSS): пример использования, основные цели и задачи, принцип работы XSS. Атака clickjacking и фишинг: цели, задачи, основные способы защиты. Обфускация (запутывание программного кода) и деобфускация: цели, задачи, примеры «запутанного» кода. Реверсивный инжиниринг (обратное проектирование): цели, задачи, основные методы. Защита объектов интеллектуальной собственности. Фундаментальные требования компьютерной безопасности. Требования классов защиты. Основные положения Руководящих документов ФСТЭК в области защиты информации. Определение и классификация несанкционированного доступа (НСД). Определение и классификация нарушителя. Модели нарушителя. Классы защищенности автоматизированных систем от несанкционированного доступа к информации.

Безопасность ресурсов сети и объектов базы данных. Безопасность ресурсов сети: средства идентификации и аутентификации, методы разделения ресурсов и технологии разграничения доступа пользователей к ресурсам сети. Монитор безопасности. Основные сетевые стандарты, протоколы взаимодействия в сетях. Модели OSI и TCP/IP. Сетевое оборудование на 2 и 3 уровнях модели OSI. Технологии обеспечения

безопасности корпоративной сети с использованием оборудования 2-го уровня модели OSI. Технологии обеспечения безопасности корпоративной сети с использованием оборудования 3-го уровня модели OSI. Анализ сетевого трафика. Wireshark. NetFlow analyzer. Построение модели угроз. Базы (словари) уязвимостей, например, CVE. Сканеры уязвимостей (Nessus). Понятие «эксплойт». Среда Metasploit framework. «Ручное» конструирование пакетов (Packet Crafting). Технологии обеспечения безопасности беспроводных сетей. Модели живучести систем и баз данных, режимы отказов - способы обнаружения и устранения. Целостность данных. Стратегии обеспечения целостности данных средствами СУБД. Средства обеспечения защиты данных от несанкционированного доступа, средства идентификации и аутентификации объектов БД, языковые средства разграничения доступа, организация аудита в системах БД. Задачи и средства администратора безопасности БД. Транзакционная целостность. Основные свойства транзакций (ACID). Технологии протоколирования (режимы undo, redo, undo/redo). Управление параллельными заданиями - последовательные расписания и механизмы блокирования (пессимистические и оптимистические стратегии).

Модели разграничения прав доступа. Модель системы безопасности HRU. Основные положения модели. Теорема об алгоритмической неразрешимости проблемы безопасности в произвольной системе. Модель распространения прав доступа Take-Grant. Расширенная модель Take-Grant и ее применение для анализа информационных потоков в автоматизированной системе (АС). Модель Белла-Лападулы как основа построения систем мандатного разграничения доступа. Основные положения модели. Базовая теорема безопасности (BST). Механизм обеспечения безопасности SELinux. Обеспечение дискреционного доступа в семействе операционных систем Windows. Обобщенные модели систем защиты информационных систем (ИС). Вероятностные модели систем защиты информации ИС. Модели безопасности ИС, построенные с использованием теории графов. Модели безопасности ИС, построенные с использованием теории автоматов.

Тема 4. Криптографические аспекты защиты информации.

Основные понятия криптографии. Основные понятия криптографии. Криптология, криптография, криптоанализ. Алфавит, текст. Шифрование, дешифрование, дешифрование. Криптосистема, криптографический шифр. Модели шифров. Блочные и поточные шифры. Понятие криптосистемы: симметричные криптосистемы, криптосистемы с открытым ключом, системы электронной подписи, управление ключами, протоколы установления подлинности (аутентификации). Симметричная криптосистема. Ключевые системы шифра. Основные требования к шифрам. Блочные шифры. Ключевая система блочных шифров. Российский стандарт ГОСТ 28147-89. Поточные шифры, гаммирование. Асимметричные криптосистемы. Алгоритм Диффи- Хеллмана. Атака «человек посередине», метод перебора, вычисление закрытого ключа, зная открытый. Шифрование методом замены (подстановки). Тест Казиски. Шифрование методом перестановки. Стеганография как один из способов обеспечения конфиденциальности и целостности информации.

Криптографические протоколы. Криптографические протоколы - основные виды и типы, область применения. Идентификация и аутентификация. Ключи криптосистемы. Жизненный цикл ключей. Требования к обеспечению безопасности жизненного цикла ключей. Управление ключами в криптографических системах. Криптографические токены.

Функции хэширования. Функции хэширования. Требования, предъявляемые к функциям хэширования. Ключевые функции хэширования. Бесключевые функции хэширования. Цифровая подпись. Общие положения. Федеральный закон «Об электронной подписи». Сертификат ключа проверки электронной подписи. Удостоверяющий центр. Функции удостоверяющего центра. Ключ проверки электронной подписи. Средства электронной подписи. Свойства электронно-цифровой подписи. Алгоритмы электронной подписи на основе эллиптических кривых ECDSA и ГОСТ Р.

3. Учебно-методическое и информационное обеспечение, включающее нормативные правовые документы, рекомендуемую литературу и Интернет-ресурсы

Нормативные акты

1. Конституция Российской Федерации. [Электронный документ]. Режим доступа: URL: http://base.consultant.ru/cons/cgi/online.cgi

2. Международный стандарт. ISO/IEC 27000:2005 Информационные технологии. Методы обеспечения безопасности. Определения и основные принципы. [Электронный документ]. Режим доступа: URL: http://www.27000.org/

3. Международный стандарт. ISO/IEC 27001:2005 Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования (BS 7799-2:2005). [Электронный документ]. Режим доступа: URL: http://www.27000.org/

4. Международный стандарт. ISO/IEC 27002:2005 Информационные технологии. Методы обеспечения безопасности. Практические правила управления информационной безопасностью. [Электронный документ]. Режим доступа: URL: http://www.27000.org/

5. Международный стандарт. ISO/IEC 27003:2005 Информационные технологии. Методы обеспечения безопасности. Руководство по внедрению системы управления информационной безопасностью. [Электронный документ]. Режим доступа: URL: http://www.27000.org/

6. Международный стандарт. ISO/IEC 27004:2005 Информационные технологии. Методы обеспечения безопасности. Измерение эффективности системы управления информационной безопасностью. [Электронный документ]. Режим доступа: URL: http://www.27000.org/

7. Международный стандарт. ISO/IEC 27005:2005 Информационные технологии. Методы обеспечения безопасности. Управление рисками информационной безопасности. [Электронный документ]. Режим доступа: URL: http://www.27000.org/

8. Международный стандарт. ISO/IEC 27006:2005 Информационные технологии. Методы обеспечения безопасности. Требования к органам аудита и сертификации систем управления информационной безопасностью. [Электронный документ]. Режим

доступа: URL: http://www.27000.org/

9. Международный стандарт. ISO/IEC 27007:2005 Информационные технологии. Методы обеспечения безопасности. Руководство для аудитора систем управления информационной безопасностью. [Электронный документ]. Режим доступа: URL: http://www.27000.org/

10. Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации» [Электронный документ]. Режим доступа: URL: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty#

Основная литература

1. Резник С. Д. Аспирант вуза: технологии научного творчества и педагогической деятельности: учебник / С. Д. Резник. — 8-е изд., перераб. и доп. — Москва: ИНФРА-М, 2022. — 388 с. — (Менеджмент в науке). - ЭБС ZNANIUM.com. - URL: https://znanium.com/catalog/product/1852167 (дата обращения: 12.01.2023). – Текст: электронный.

2. Аникин В. М. Диссертация в зеркале автореферата: Методическое пособие для аспирантов и соискателей ученой степени естественно-научных специальностей: методическое пособие / В. М. Аникин, Д. А. Усанов. – Москва: ООО "Научно-издательский центр ИНФРА-М", 2019. - 128 с. – ЭБС ZNANIUM.com. – URL: http://znanium.com/go.php?id=1008538 (дата обращения: 12.01.2023). - Текст: электронный.

Дополнительная литература

1. Козьминых С. И. Обеспечение комплексной защиты объектов информатизации: учебное пособие для студентов вузов / С. И. Козьминых; Финуниверситет. – Москва: Юнити-Дана, 2020. - 544 с. - Текст: непосредственный. - То же. - ЭБС ZNANIUM.com. - URL: https://znanium.com/catalog/product/1359079 (дата обращения: 12.01.2023). - Текст: электронный.

2. Козьминых С. И. Организационное и правовое обеспечение информационной безопасности: учебное пособие / С. И. Козьминых. - Тбилиси: Справедливая Грузия, 2020. - 309 с. - ЭБС ZNANIUM.com. - URL: https://znanium.com/catalog/product/1359091 (дата обращения: 12.01.2023). – Текст: электронный.

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. Электронная библиотека Финансового университета (ЭБ) http://elib.fa.ru/
2. Электронно-библиотечная система BOOK.RU http://www.book.ru
3. Электронно-библиотечная система «Университетская библиотека ОНЛАЙН» http://biblioclub.ru/
4. Электронно-библиотечная система Znanium http://www.znanium.com
5. Электронно-библиотечная система издательства «ЮРАЙТ» https://www.biblio-online.ru/
6. Электронно-библиотечная система издательства «Лань» https://e.lanbook.com/
7. Деловая онлайн-библиотека Alpina Digital http://lib.alpinadigital.ru/
8. Научная электронная библиотека eLibrary.ru http://elibrary.ru
9. Национальная электронная библиотека http://нэб.рф/
10. Минобрнауки.рф - Сайт Министерства образования и науки России
11. http://vak.ed.gov.ru/ - сайт Высшей аттестационной комиссии Минобрнауки России
12. http://www.rsl.ru/ru/s2/d104/ - Сайт Российской государственной библиотеки (фонд диссертаций)

4. Критерии балльной оценки

Критерии оценки знаний в ходе ответов на теоретические вопросы:

«Отлично» соответствует ответу на теоретический вопрос экзаменационного билета, при котором глубоко и полно раскрыты теоретические и практические аспекты вопроса, проявлен самостоятельный подход к его изложению и продемонстрировано

понимание дискуссионное™ данной проблематики, а также даны полные ответы на дополнительные вопросы.

«Хорошо» соответствует ответу на теоретический вопрос экзаменационного билета, при котором коротко освещены узловые моменты вопроса, вызывают затруднения более глубокое обоснование основных положений и/или ответы на дополнительные вопросы по данной проблематике.

«Удовлетворительно» соответствует ответу, при котором частично раскрыты основные положения вопроса, есть ошибки в ответах на основные и/или дополнительные вопросы, нарушена логика изложения.

Оценка «неудовлетворительно» выставляется в случае, если материал излагается непоследовательно, не аргументированно, бессистемно, ответы на вопросы выявили несоответствие уровня знаний в части формируемых компетенций по дисциплине, направленной на подготовку к сдаче кандидатского экзамена.

Перед процедурой обсуждения ответов, экзаменующихся каждый член экзаменационной комиссии, выставляет свою персональную оценку для каждого аспиранта, при этом итоговая оценка представляет среднее арифметическое от суммы оценок, выставленных каждым членом комиссии.

Перечень примерных вопросов для сдачи кандидатского экзамена

Общетеоретические.

1. Основные требования к обеспечению информационной безопасности в информационных системах.

2. Обеспечение безопасности информационных ресурсов, государственных информационных ресурсов.

3. Нормативно-правовое обеспечение информационной безопасности информационных систем.

4. Обзор Российского и международного (ведущих стран) законодательства в сфере защиты информации в информационных системах.

5. Базовые проблемы защиты информации в информационных системах.

6. Аспекты защиты коммерческой тайны, предотвращение промышленного шпионажа.

7. Сведения, составляющие банковскую тайну. Обеспечение безопасности банковской тайны.

8. Аспекты защиты авторского права. Правовая база в сфере защиты банковской тайны.

9. Определение и классификация компьютерных атак и особенности их обнаружения.

10. Модель угроз безопасности информации в информационных системах. Меры по обеспечению безопасности информации.

11. Принципы и основы построения систем защиты информации (СЗИ) в информационных системах.

12. Нормативная, методическая и научная базы системы защиты информации в информационных системах.

13. Инструментальный базис обеспечения информационной безопасности информационных систем.

14. Основополагающие принципы разработки и построения систем обеспечения информационной безопасности информационных систем.

15. Нормативно-правовая документация по обеспечению информационной безопасности информационных систем: основные требования, содержание, структура и обоснование.

16. Структура, цели и задачи регуляторов (органов), выполняющих и обеспечивающих информационную безопасность информационных систем.

17. Организационный и правовой статусы службы информационной безопасности информационной системы.

18. Организационные, технические и режимные меры обеспечения информационной безопасности информационных систем.

19. Разграничение прав доступа к защищаемой информации в информационной системе. Разработки и обоснование политики безопасности.

20. Аспекты организации защищённого делопроизводства и мероприятий по защите информационной безопасности информационных систем.

21. Технические методы и средства защиты информации в информационных системах и на объектах информатизации.

22. Сжатие данных. Обнаружение и коррекция ошибок при передаче данных.

23. Классификация сигналов: непрерывные, дискретные, квантованные по уровню, цифровые сигналы.

24. Кодирование информации, эффективное кодирование информации. Кодирование как средство обеспечения целостности информации. Примеры алгоритмов кодирования.

25. Программно-аппаратная база обеспечения информационной безопасности информационных систем и средства ограничения доступа к компонентам информационной системы.

Вопросы, соответствующие содержанию области исследования.

1. Классификация видов несанкционированного доступа и основные условия функционирования средств защиты информации.

2. Средства противодействия локальному несанкционированному доступу к информации в информационной системе.

3. Задачи и требования к техническим средствам защиты информации для обеспечения конфиденциальности информации.

4. Системный анализ базовых проблем инженерно-технической защиты информации в информационных системах.

5. Классификация способов и средств организационных и технических мер защиты информации в информационных системах.

6. Условия и принципы утечки информации. Структура технического канала

утечки информации. Классификация каналов утечки информации. Основные характеристики технических каналов утечки информации.

7. Акустический канал утечки информации. Основные функции и принципы действия технических средств акустической (речевой) разведки.

8. Средства защиты от утечки по акустическому каналу. Деконспирационные признаки. Непосредственное прослушивание звуковой информации и прослушивание информации направленными микрофонами.

9. Принцип работы телефона и микрофона. Построение системы защиты от негласной записи информации на диктофон.

10. Виброакустический канал утечки информации. Построение системы защиты информации от утечки по вибрационному каналу. Лазерные системы съема, электронные стетоскопы и гидроакустические преобразователи.

11. Радиоэлектронный канал утечки информации. Общая характеристика и особенности радиоэлектронной разведки. Перехват информации с радиотелефонов, офисной техники, кабелей, проходящих через помещение.

12. Определение радиозакладок. Основные характеристики и основные элементы радиозакладок. Прослушивание информации с помощью внедрённых радиозакладок.

13. Электромагнитный канал утечки информации. Активная и пассивная защита информации. Прослушивание информации с помощью пассивных закладок. Приёмники информации с радиозакладок.

14. Технические методы и средства поиска работающих радиозакладок. Применение нелинейных радиолокаторов для поиска радиозакладок.

15. Телефонная линия как один из основных каналов утечки информации. Контактный и бесконтактный способы съёма информации с помощью телефонных линий: непосредственное подключение, считывание с помощью трансформаторов, преобразователей Холла, индуктивных датчиков.

16. Принцип действия телефонного аппарата, беззаходовый несанкционированный съем информации, несанкционированное использование микрофона телефонного аппарата, телефонные ретрансляторы.

17. Защита от несанкционированного съёма информации в радиоэлектронных каналах. Устройства уничтожения закладных устройств. Устройства предотвращения утечки информации по телефонному каналу. Предотвращение утечки информации по сотовым сетям связи.

18. Электромагнитный канал утечки информации. Низкочастотные и высокочастотные устройства съёма информации. Системы защиты информации от утечки по электромагнитный каналу.

19. Оптический канал утечки информации. Телевизионные системы наблюдения.

20. Построение, анализ и оценка структурных, функциональных, информационных и комплексных моделей каналов утечки информации.

21. Построение, анализ и оценка моделей систем защиты. Оценка эффективности модели защиты, выбор оптимальной системы защиты информации и выбор соответствующих технических средств защиты информации.

22. Технический контроль и оценка эффективности мер защиты информации. Назначения, средства, содержание и методы технического контроля.

23. Защита программного обеспечения от разрушающих программных воздействий (программных закладок, вирусов) и от реверсивного инжиниринга.

24. Описание взаимодействия прикладной программы и программной закладки. Методы внедрения программных закладных устройств.

25. Модель изолированной программной среды. Методы верификации защитных механизмов от закладных устройств.