МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФГБОУ ВО «Брянский государственный технический университет» (БГТУ)

Факультет информационных технологий
(наименование факультета/института)
Системы информационной безопасности
(наименование кафедры, ответственной за реализацию дисциплины)

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 00AE9AA1E2F51D554BB517B57D9399435E
Владелец: Шкаберин Виталий Александрович
Действителен: с 04.07.2023 до 26.09.2024

УТВЕРЖДАЮ
Первый проректор
по учебной работе и цифровизации
_____ В.А. Шкаберин
«___» _____ 2022 г.

ПРОГРАММА КАНДИДАТСКОГО ЭКЗАМЕНА ПО СПЕЦИАЛЬНОЙ ДИСЦИПЛИНЕ

Методы и системы защиты информации, информационная безопасность
(наименование дисциплины)

2.3.6. Методы и системы защиты информации, информационная безопасность
(код и наименование научной специальности)

Технические науки
(наименование отрасли наук)

высшее образование – подготовка кадров высшей квалификации
(уровень образования)

Очная
(форма обучения)

2022
(год набора)

Брянск 2022

Программа кандидатского экзамена по специальной дисциплине

Методы и системы защиты информации, информационная безопасность

(наименование дисциплины)

2.3.6. Методы и системы защиты информации, информационная безопасность

(код и наименование научной специальности)

Разработал:

Заведующий кафедрой «СИБ», к.т.н., доцент		М.Ю. Рытов
(должность, ученая степень, ученое звание)	*(подпись)*	*(И.О. Фамилия)*

Рассмотрена и одобрена на заседании кафедры Системы информационной безопасности

(наименование кафедры, ответственной за реализацию дисциплины)

«25» марта 2022 г., протокол № 7

Заведующий кафедрой к.т.н., доцент		М.Ю. Рытов
(ученая степень, ученое звание)	*(подпись)*	*(И.О. Фамилия)*

ПРЕДИСЛОВИЕ

Программа кандидатского экзамена предназначена для сдачи аспирантами кандидатского экзамена по специальной дисциплине «Методы и системы защиты информации, информационная безопасность» по программе аспирантуры по научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

1. ЦЕЛЬ И ЗАДАЧИ ПРОВЕДЕНИЯ КАНДИДАТСКОГО ЭКЗАМЕНА

Цель кандидатского экзамена – установить глубину профессиональных знаний аспиранта, уровень подготовленности к самостоятельной научно-исследовательской работе.

Задачи:

- выявить уровень теоретической и профессиональной подготовки аспиранта;

- оценить знания в области анализа и синтеза современных методов и систем защиты информации, теории и принципов их построения.

2. МЕСТО КАНДИДАТСКОГО ЭКЗАМЕНА В СТРУКТУРЕ ПРОГРАММЫ АСПИРАНТУРЫ

Кандидатский экзамен по специальной дисциплине является промежуточной аттестацией дисциплины «Методы и системы защиты информации, информационная безопасность» относится к образовательному компоненту программы аспирантуры и реализуется на 3 курсе в 1 семестре.

3. ОБЪЕМ КАНДИДАТСКОГО ЭКЗАМЕНА

Общая трудоемкость кандидатского экзамена по специальной дисциплине составляет 1 зачетная единица (36 академических часа).

4. СОДЕРЖАНИЕ ПРОГРАММЫ КАНДИДАТСКОГО ЭКЗАМЕНА

4.1. Структура программы кандидатского экзамена

Структура программы кандидатского экзамена по специальной дисциплине представлена в виде тематического плана в таблице 1.

Таблица 1 – Тематический план кандидатского экзамена

№ п/п	Наименование раздела дисциплины	Содержание раздела (дидактические единицы)
1	Теория и методология информационной безопасности	Проблемы развития теории и практики обеспечения информационной безопасности. Терминология, определяющая научную и предметную основу и характер деятельности по обеспечению информационной безопасности. информационные проблемы современного общества. Составляющие информационной безопасности. национальные интересы РФ в информационной сфере. Проблемы и перспективы международного сотрудничества в области ИБ. Понятие и сущность защиты информации. Цели защиты информации. Концептуальная модель информационной безопасности. Предмет защиты информации. информация как объект права собственности. Объект защиты информации. Случайные угрозы. Преднамеренные угрозы. Модель гипотетического нарушителя информационной безопасности. Основные принципы построения системы защиты. методы защиты информации. Минимизация ущерба, дублирование, повышение надежности. Создание отказоустойчивых информационных систем. Оптимизация взаимодействия. Методы и средства ЗИ от традиционного шпионажа и диверсий. Методы и средства защиты от ПЭМИН. Защита от НСД. Модели защиты информации. Криптографические методы ЗИ.
2	Математическое моделирование процессов защиты информации	Определения математической модели и математического моделирования. Требования, предъявляемые к математическим моделям. Области применения математических моделей. Классификация математических моделей по типам, свойствам и назначению. Методы моделирования сложных систем. Общие принципы и средства построения математических моделей процессов защиты информации. Способы построения детерминированных математических моделей. Аналитические и численные методы решения уравнений. Визуализация результатов моделирования. Построение математических моделей на основе экспериментальных данных. Применение корреляционного, регрессионного и дисперсионного анализов. Условия применимости статистического анализа. Оценка достоверности и точности математических моделей.

3	Организационно-правовая защита информации	Обзор нормативно-правовой базы РФ в области обеспечения информационной базы. Общая характеристика организационных методов защиты информации. Требования к построению систем безопасности предприятия. Концептуальная модель информационной безопасности. Виды объектов защиты. Классификация угроз информационной безопасности и виды каналов утечки информации на предприятии. Основные направления организационной защиты информации на предприятии. Характеристика защитных действий. разглашение защищаемой информации. Способы пресечения разглашения защищаемой информации. Противодействие несанкционированному доступу к информации. Государственная тайна и порядок отнесения к ней информации. Защита государственной тайны. Организация режима секретности, его особенности и содержание. Коммерческая тайна и порядок её определения. Организация работ с информацией, составляющей коммерческую тайну. Организация и обеспечение защиты коммерческой тайны на предприятии. Организация инженерно-технической безопасности. Организация безопасности функционирования информационных систем. Проведение аналитико-разведывательной работы. Организационная структура службы безопасности. Организация внутриобъектового режима на предприятия. Организация охраны объектов предприятия. Организация и обеспечение защиты коммерческой тайны на предприятии. Организация инженерно-технической безопасности. Организация безопасности функционирования информационных систем. Проведение аналитико-разведывательной работы. Цели и задачи информационно-аналитической работы. Направления и методы аналитической работы. Этапы выполнения информационно-аналитических исследований производственных ситуаций. Методы выполнения аналитических исследований. Основы конкурентной разведки. Подбор и подготовка кадров. Проверка персонала на благонадежность. Заключение контрактов и соглашений о секретности. Особенности увольнения сотрудников, владеющих конфиденциальной информацией. Подбор и подготовка кадров. Проверка персонала на благонадежность. Заключение контрактов и соглашений о секретности. Особенности увольнения сотрудников, владеющих конфиденциальной информацией. Правовая основа системы лицензирования и сертификации в РФ. Лицензирование деятельности по защите информации. Сертификация средств защиты информации.

4	Инженерно-техническая защита информации	Виды угроз безопасности информации, защищаемой техническими средствами. Принципы добывания и обработки информации техническими средствами. Органы добывания информации. Принципы ведения разведки. Технология добывания информации. Способы доступа к конфиденциальной информации. Добывание информации без физического проникновения в контролируемую зону. Доступ к источникам информации без нарушения государственной границы. Показатели эффективности разведки. Особенности утечки информации по техническим каналам. Характеристики технических каналов утечки информации. Оптические каналы утечки информации. Радиоэлектронные каналы утечки информации. Акустические каналы утечки информации. Материально-вещественные каналы утечки информации. Комплексное использование каналов утечки информации. Основные способы и принципы работы средств наблюдения объектов, подслушивания и перехвата сигналов. Способы и средства наблюдения: способы и средства наблюдения в оптическом диапазоне, способы и средства наблюдения в радиодиапазоне. Способы и средства перехвата сигналов. Способы и средства подслушивания. Способы и средства добывания информации о радиоактивных веществах. Виды и природа каналов утечки информации при эксплуатации ЭВМ. Анализ возможности утечки информации через ПЭМИ. Способы обеспечения ЗИ от утечки через ПЭМИН опасных сигналов акустоэлектрических преобразователей; экранирование и компенсация информативных полей. Подавление информативных сигналов в цепях заземления и электропитания. Подавление опасных сигналов. Принципы защиты информации. Основные методы защиты информации техническими средствами. способы и принципы работы средств защиты информации от наблюдения, подслушивания и перехвата. Способы и средства противодействия наблюдению. Способы и средства противодействия подслушиванию. Способы и средства предотвращения записи речи на диктофон. Способы и средства предотвращения записи речи через закладные устройства. Защита информации в каналах связи. Разработка инженерно-технической системы защиты информации объекта. Системный подход к инженерно-технической защите информации. Основные этапы проектирования системы защиты информации техническими средствам. Принципы моделирования объектов защиты и технических каналов утечки информации. Рекомендации по выбору методов и средств инженерно-технической защиты информации. Способы оценки угроз безопасности информации и расходов на техническую защиту. САПР систем инженерно-технической защиты информации. Задачи и место инженерно-технической охраны в системе обеспечения информационной безопасности. Структура системы инженерной защиты и технической охраны объектов. Средства инженерной защиты. Роль и место технических средств в организации режима охраны. Современная концепция защиты объектов. Основные составляющие систем ТСО: датчики, приборы визуального наблюдения, системы сбора и обработки информации, средства связи, питания и тревожно-вызывной сигнализации. Практическая реализация систем ТСО: охрана режимных помещений, проект охраны объектов. Современные систем видеонаблюдения: структура и функции. Нормативно-правовая база инженерно-технической защиты информации. Организационные и технические меры инженерно-технической защиты информации в государственных и коммерческих структурах. Лицензирование деятельности и сертификация средств защиты информации. Аттестация объек-

5	Программно-аппаратная защита информации	Основные понятия: объект защиты информации, компьютерная система, безопасность информации в КС, система защиты информации. Уязвимость компьютерных систем. Искусственные и естественные угрозы. Каналы утечки информации. Политика безопасности в компьютерных системах. Избирательная политика безопасности. Управление информационными потоками. Оценка защищенности. механизмы защиты. Система документов России. Основные понятия и концепции. Идентификация и аутентификация пользователя. Типовые схемы идентификации и аутентификации пользователя. Особенности применения пароля для аутентификации пользователя. Биометрическая идентификация и аутентификация пользователя. Взаимная проверка подлинности пользователей. Протоколы идентификации с нулевой передачей знаний. Упрощенная схема идентификации с нулевой передачей знаний. Параллельная схема идентификации с нулевой передачей знаний. Схема идентификации гиллоу-куискуотера. Защита информации в КС от несанкционированного доступа. Система разграничения доступа к информации в КС. Управление доступом. Состав системы разграничения доступа. Концепция построения систем разграничения доступа. Организация доступа к ресурсам КС. Обеспечение целостности информации в КС. Полностью контролируемые компьютерные системы. Программная реализация функций КС. Аппаратная реализация функций КС. Частично контролируемые компьютерные системы. Основные элементы и средства защиты от несанкционированного доступа. Защита информации в ПЭВМ. Категории средств защиты информации. Защита информации, обрабатываемой ПЭВМ и ЛВС, от утечки по сети электропитания. Виды мероприятий по защите информации. Современные системы защиты ПЭВМ от несанкционированного доступа к информации. Методы, затрудняющие считывание скопированной информации. Методы, препятствующие использованию скопированной информации. Основные функции средств защиты от копирования. Основные методы защиты от копирования. Классификация средств исследования программ. Методы защиты программ от исследования. Анализ программ на этапе их эксплуатации. Общая характеристика и классификация компьютерных вирусов. Общая характеристика средств нейтрализации компьютерных вирусов. Классификация методов защиты от компьютерных вирусов.

6	Криптографическая защита информации	Алгебраические модели шифров. Модель Шеннона. Понятие шифрвеличины и шифробозначения. Опорный шифр. Детерминированные и стохастические генераторы ключевого потока. Вероятностные модели шифров. Шифры с ограниченным и неограниченным ключом. Открытые сообщения. Алфавиты сообщений. Частотные характеристики сообщений. Избыточность. Математические модели открытых текстов. Критерии распознавания. Цепи Маркова. Энтропия и избыточность языка. Расстояние единственности. Стойкость шифров. Теоретическая стойкость шифров. Практическая стойкость шифров. Теоретико-информационный подход к оценке криптостойкости шифров. Надежность ключей и сообщений. Совершенные шифры. Безусловно стойкие и вычислительно стойкие шифры. Рабочая характеристика шифра. Сложность взлома. Аппаратные и термодинамические ограничения. Китайская лотерея. Эквивалентная устойчивость к лобовому вскрытию симметричных и ассиметричных ключей. Принципы рассеивания и перемешивания. Имитостойкость шифров. Имитация и подмена сообщения. Способы обеспечения имитостойкости. Коды аутентификации. Помехостойкость шифров. Шифры, не распространяющие искажений типа "замена знаков". Шифры, не распространяющие искажений типа "пропуск-вставка знаков". Практические вопросы повышения надежности. Принципы построения блочных шифров. Применяемые математические преобразования (операции). Лавинный эффект, диффузия и конфузия. Сеть Файстеля. Матричные преобразования. Современные блочные криптоалгоритмы. Размер блока, размер ключа, количество раундов. Режимы использования блочных шифров. Принципы построения поточных шифрсистем. Управляющие и шифрующие блоки. Генераторы ключевого потока. Истинно случайные и псевдослучайные последовательности. Синхронизация поточныхшифрсистем. Регистры сдвига с обратной связью. Алгоритм Берленкемпа-Месси. Усложнение линейных рекуррентных последовательностей. Примеры поточных шифрсистем. Теоремы об однонаправленной функции и однонаправленной функции с лазейкой. Шифрсистема RSA. Вопросы практической реализации RSA. Взаимосвязь компонентов RSA. Шифрсистема Эль-Гамаля. Вопросы практической реализации шифрсистемы Эль-Гамаля. Шифрсистемы на основе помехоисправляющих кодов Шифрсистема Мак-Элиса. Шифрсистемы на основе маскировки задач полиномиальной сложности. Рюкзачные шифрсистемы. Требования к криптографическим хэш-функциям. Блочно-итерационные и шаговые функции. Ключевые хэш-функции, коды аутентичности сообщений. Бесключевые хэш-функции, коды обнаружения ошибок. Схемы применения ключевых и бесключевых хэш-функций. Современные алгоритмы хеширования. Сравнение свойств собственноручной и цифровой подписи. Цифровые подписи на основе шифрсистем с открытыми ключами. Цифровая подпись Фиата - Шамира. Цифровая подпись Эль-Гамаля. Одноразовые цифровые подписи. Современные алгоритмы цифровой подписи. Протоколы распределения ключей. Передача ключей с использованием симметричного шифрования. Передача ключей с использованием асимметричного шифрования. Открытое распределение ключей. Предварительное распределение ключей. Способы установления ключей для конференц-связи. Схемы разделения секрета. Доказательства с нулевым разглашением. Подбрасывание монеты по телефону. Электронные деньги. Абонентское и канальное шифрование. Области приме-

7	Защита персональных данных	Основные нормативно-правовые акты в области защиты персональных данных. Требования ФЗ «О персональных данных». Понятийный аппарат. Обеспечение конфиденциальности персональных данных. Специальные категории персональных данных. Право субъекта персональных данных на доступ к своим персональным данным. Принципы обработки и хранения персональных данных. Условия обработки персональных данных: согласие субъекта на обработку, обрабатываемые без уведомления персональных данных. Особенности обработки персональных данных в государственных или муниципальных информационных системах персональных данных. Основные нормативно-правовые акты в области защиты персональных данных за рубежом. Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных от 28.01.1981 EST № 108. Федеральные органы, уполномоченные в области обеспечения безопасности персональных данных– регуляторы. Сфера деятельности регуляторов.. Понятие информационной системы персональных данных. Условий создания и использования персональных данных: состав персональных данных и цель их обработки; технология обработки; субъекты, создающие и потребляющие персональных данных; правила доступа; используемые объекты. Формы представления персональных данных: акустическая (речевая) информация; видовая информация; информация в виде сигналов; информация в виде логических структур. Техническая структура информационной системы персональных данных: технические средства, используемые каналы связи, программные средства. Информационные потоки, циркулирующие в информационной системе персональных данных. Граничное телекоммуникационное оборудование и виртуальные локальные сети. Характеристик безопасности персональных данных: конфиденциальность, целостность и доступность. Классификационные признаки уровней защищенности испдН: тип угрозы, количество субъектов ПДн, тип ИС. таблица определения уровней защищенности ИСПДн. Классификация угроз безопасности персональных данных. Анализ и характеристики угроз возможной утечки информации по техническим каналам. Анализ и характеристики угроз несанкционированного доступа к информации в информационной системе персональных данных, включая характеристики источников угроз несанкционированного доступа, характеристики уязвимостей системного и прикладного программного обеспечения, характеристики угроз безопасности персональных данных, реализуемых с использованием протоколов межсетевого взаимодействия и программно-математических воздействий, характеристики нетрадиционных информационных каналов и результатов несанкционированного или случайного доступа. Типовые модели угроз безопасности персональных данных, обрабатываемых в информационных системах (автоматизированных рабочих местах, локальных и распределенных информационных системах), не имеющих и имеющих подключение к сетям связи общего пользования и (или) сетям международного информационного обмена.

8	Управление интеллектуальной собственностью	Основные принципы авторского и патентного права. Объекты права. Имущественные и личные права. Способы гражданско-правовой защиты. Средства индивидуализации. Охрана нетрадиционных объектов. Защита авторских и смежных прав. Защита промышленной собственности. Защита программ для ЭВМ и баз данных. Защита служебной и коммерческой тайны. Защита рационализаторских предложений. Международная патентная система. Всемирная организация интеллектуальной собственности.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ КАНДИДАТСКОГО ЭКЗАМЕНА

5.1. Перечень основной и дополнительной учебной литературы:

а) основная литература

1. Астайкин А.И. Методы и средства обеспечения программно-аппаратной защиты информации [Электронный ресурс] : научно-техническое издание / А.И. Астайкин [и др.]. — Электрон. текстовые данные. — Саров: Российский федеральный ядерный центр – ВНИИЭФ, 2015. — 224 c. — 978-5-9515-0305-3. — Режим доступа: http://www.iprbookshop.ru/60959.html

2. Коваленко Ю.И. Методика защиты информации в организациях [Электронный ресурс] : монография / Ю.И. Коваленко, Г.И. Москвитин, М.М. Тараскин. — Электрон. текстовые данные. — М. : Русайнс, 2016. — 162 c. — 978-5-4365-0887-0. — Режим доступа: http://www.iprbookshop.ru/61625.html

3. Свинарев Н.А. Инструментальный контроль и защита информации [Электронный ресурс] : учебное пособие / Н.А. Свинарев [и др.]. — Электрон. текстовые данные. — Воронеж: Воронежский государственный университет инженерных технологий, 2013. — 192 c. — 978-5-00032-018-1. — Режим доступа: http://www.iprbookshop.ru/47422.html

б) дополнительная литература

1) Аверченков В.И. Методы и средства инженерно-технической защиты информации [Электронный ресурс] : учебное пособие / В.И. Аверченков [и др.]. — Электрон. текстовые данные. — Брянск: Брянский государственный технический университет, 2012. — 187 c. — 5-89838-357-3. — Режим доступа: http://www.iprbookshop.ru/7000.html

2) А. Джейсон Защита данных. От авторизации до аудита. [Электронный ресурс] — СПб.: Питер, 2021. — 272 с.: (Серия «Для профессионалов»). ISBN 978-5-4461-1733-8. — Режим доступа: https://lib.fbtuit.uz/assets/files/_____.pdf

3) Паренти, Томас. Кибербезопасность : что руководителям нужно знать и делать : / Томас Паренти, Джек Домет. – 2-е изд.. – Москва : Манн, Иванов и Фербер, 2022. ISBN 978-5-00195-484-2 — Режим доступа: https://humpty.ru/book/17547-kiberbezopasnost-chto-rukovoditeliam-nuzhno-znat-i-delat

4) М. Саттон, А. Гринн Fuzzing : исследование уязвимостей методом грубой силы – Санкт-Петербург ; Москва, 2017. - 555 с. (High tech).; ISBN —

Режим доступа: 978-5-93286-147-9https://codeby.net/attachments/satton-m-fuzzing-issledovanie-ujazvimostej-metodom-gruboj-sily-pdf.27608/

5) А. А. Бирюков Информационная безопасность: защита и нападение, 2-е издание – Москва, 2017. - 474 с. ISBN 978-5-94074-647-8 — Режим доступа: https://vk.com/wall-49131654_93473

6) Организационно-правовое обеспечение информационной безопасности [Текст] : монография / А. В. Морозов, Т. А. Полякова ; Федеральное гос. бюджетное образовательное учреждение высш. проф. образования "Российская правовая акад. М-ва юстиции Российской Федерации". - Москва, 2017. – 273 с., ISBN 978-5-89172-544-7— Режим доступа: https://vk.com/wall-43363264_525959

5.2. Перечень ресурсов сети «Интернет», необходимых для подготовки к сдаче кандидатского экзамена:

1.Единое окно доступа к информационным ресурсам (http://window.edu.ru).

2. Национальная электронная библиотека (http://www.elibrary.ru).

3. Федеральное хранилище «Единая коллекция цифровых образовательных ресурсов» (http://school-collection.edu.ru).

4. Федеральный Интернет-портал «Российское образование» (http://www.edu.ru).

5. Электронно-библиотечная система «IPRbooks» (http://www.iprbookshop.ru).

6. Электронно-библиотечная система «Лань» (https://e.lanbook.com).

7. Сайт ФГБУ Федеральный институт промышленной собственности http://www1.fips.ru.

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДЛЯ ПРОВЕДЕНИЯ КАНДИДАТСКОГО ЭКЗАМЕНА

Для обеспечения проведения кандидатского экзамена имеется следующая материально-техническая база:

– учебная аудитория, оснащенная комплектом мебели и доской, для проведения консультаций и кандидатского экзамена;

– компьютерные классы с постоянным доступом к информационно-телекоммуникационной сети «Интернет», а также читальные залы научной библиотеки БГТУ для самостоятельной работы аспирантов.

7. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ПРОВЕДЕНИЯ КАНДИДАТСКОГО ЭКЗАМЕНА ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Проведение кандидатского экзамена для аспирантов с ограниченными возможностями здоровья проводится с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья.

При проведении промежуточной аттестации обеспечивается соблюдение следующих требований:

- для аспирантов из числа лиц с ограниченными возможностями здоровья промежуточная аттестация проводится с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся (далее - индивидуальные особенности);

- проведение мероприятий по промежуточной аттестации для лиц с ограниченными возможностями здоровья в одной аудитории совместно с аспирантами, не имеющими ограниченных возможностей здоровья, допускается, если это не создает трудностей для аспирантов;

- присутствие в аудитории ассистента, оказывающего аспирантам необходимую техническую помощь с учетом их индивидуальных особенностей (занять рабочее место, понять и оформить задание, общаться с преподавателем);

- предоставление аспирантам при необходимости услуги с использованием русского жестового языка, включая обеспечение допуска на объект сурдопереводчика, тифлопереводчика (в организации должен быть такой специалист в штате (если это востребованная услуга) или договор с организациями системы социальной защиты по предоставлению таких услуг в случае необходимости);

- предоставление аспирантам права выбора последовательности выполнения задания и увеличение времени выполнения задания (по согласованию с преподавателем);

- по желанию аспиранта устный ответ при контроле знаний может проводиться в письменной форме или наоборот, письменный ответ заменен устным.

8. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ АСПИРАНТОВ

Сдача аспирантом кандидатского экзамена по специальной дисциплине «Методы и системы защиты информации, информационная безопасность» относится к оценке результатов освоения дисциплины «Методы и системы защиты информации, информационная безопасность», осуществляемой в рамках промежуточной аттестации.

Для приема кандидатского экзамена по специальной дисциплине создается экзаменационная комиссия. Регламент работы экзаменационной комиссии определяется Положением об экзаменационной комиссии и порядке приема кандидатских экзаменов в БГТУ.

Шкала оценивания

Уровень знаний аспиранта определяется оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Показатели и критерии оценивания промежуточной аттестации

Оценка «отлично» - аспирант дает полные, исчерпывающие и аргументированные ответы; грамотно использует научную терминологию; умеет связывать теорию с практикой, высказывать и обосновывать свои суждения. Во вре-

мя экзамена аспирант должен подробно ответить на три вопроса экзаменационного билета.

Оценку «хорошо» - аспирант дает достаточно полные и аргументированные ответы; применяет научную терминология, но при этом допускает ошибку или неточность в определениях, понятиях; умеет связывать теорию с практикой, высказывать и обосновывать свои суждения. Во время экзамена аспирант должен подробно ответить на три вопроса экзаменационного билета. Допускаются незначительные недочеты и неточности, которые аспирант исправляет самостоятельно в процессе беседы с экзаменационной комиссией.

Оценку «удовлетворительно» - аспирант дает неполные и слабо аргументированные ответы; допускает существенные терминологические неточности; частично аргументирует собственную позицию или точку зрения. Во время экзамена аспирант должен подробно ответить на один вопрос экзаменационного билета и частично на два других вопроса.

Оценку «неудовлетворительно» - отмечается отсутствие знания терминологии, научных оснований, признаков, характеристик рассматриваемой проблемы; не представлена собственная точка зрения по данному вопросу. Во время экзамена аспирант частично отвечает на вопросы.

8.1. Контрольно-измерительные материалы для промежуточной аттестации (сдача кандидатского экзамена) аспирантов

8.1.1. Вопросы для промежуточной аттестации

Раздел «Теория и методология информационной безопасности»

1. Понятие информационной безопасности, основные составляющие информационной безопасности.
2. Источники угроз информационной безопасности РФ и их классификация.
3. Определение защиты информации, безопасности информации
4. Политика безопасности и анализ рисков;
5. Сущность информации как объекта права собственности.
6. Раскройте сущность объекта защиты.
7. Классификация угроз информационной безопасности, основные группы классификации.
8. Модель нарушителя информационной безопасности?
9. Основные принципы построения системы защиты информации.
10. Основные модели защиты информации и их особенности.
11. Сущность методов защиты от случайных уг роз
12. Понятия идентификации и аутентификации, основные виды аутентификации.
13. Повышение надежности и отказоустойчивости информационных систем.
14. Особенность построения защиты от несанкционированного доступа

Раздел «Математическое моделирование процессов защиты информации»

15. Определения математической модели и математического моделирования.
16. Требования, предъявляемые к математическим моделям.
17. Области применения математических моделей.
18. Классификация математических моделей по типам, свойствам и назначению.
19. Способы построения детерминированных математических моделей.
20. Аналитические и численные методы решения уравнений.
21. Сущность методов моделирования сложных систем.
22. Общие принципы и средства построения математических моделей процессов защиты информации.
23. Особенности построения математических моделей процессов защиты информации на основе экспериментальных данных.
24. Понятия корреляционного, регрессионного и дисперсионного анализов. Условия применимости статистического анализа.
25. Оценка достоверности и точности математических моделей.
26. Понятия целевой функции, оптимизируемых и фиксированных параметров, ограничений при оптимизации.
27. Понятие одномерной оптимизации. Глобальные и локальные экстремумы. Условия оптимума дифференцируемой функции одной переменной.
28. Понятие многомерной безусловной оптимизации. Условия оптимума дифференцируемой функции нескольких переменных.

Раздел «Организационно-правовая защита информации»

29. Общая характеристика организационных методов защиты информации.
30. Основные принципы организации системы безопасности объекта. Модель комплексной системы безопасности.
31. Классификация угроз информационной безопасности. Виды КУИ.
32. Основные направления организационной защиты информации на объекте.
33. Виды каналов несанкционированного доступа к информации. Их характеристика.
34. Концептуальная модель информационной безопасности.
35. Требования к построению систем безопасности предприятия.
36. Цели и задачи системы безопасности объекта. Виды объектов защиты.
37. Характеристика типовой структуры службы безопасности.
38. Случаи разглашение защищаемой информации.
39. Основные задачи службы безопасности объекта.
40. Характеристика функций службы безопасности объекта.
41. Права, обязанности и ответственность сотрудников службы безопасности.
42. Организация режима и охраны на объекте. Основные задачи.

43. Виды пропускных документов.
44. Порядок организации пропускного режима.
45. Организация охраны стационарных объектов.
46. Основные задачи охраны объектов.
47. Виды охраны стационарных объектов.
48. Характеристика деятельности отдела кадров объекта с позиции обеспечения защиты информации.
49. Способы пресечения разглашения защищаемой информации.
50. Организация инженерно-технической защиты объектов.
51. Характеристика организационных, организационно-технических и технических мероприятий защиты информации на объекте.
52. Организация аттестации защищенных помещений.
53. Организация работ по защите информации отдела обеспечения внешней деятельности.
54. Персонал фирмы и его роль в утечке информации.
55. Основные принципы организации профессионального отбора персонала.
56. Основные рекомендации при организации проверки и отбора кандидатов на работу в коммерческие предприятия.
57. Характеристика процесса увольнения кадров из коммерческих структур.
58. Особенности увольнения сотрудников, владеющих конфиденциальной информацией.
59. Основные этапы и процедуры профотбора персонала на коммерческие предприятия
60. Понятие режима секретности, его содержание и особенности.
61. РСО, ПДТК и их полномочия.
62. Порядок работы с секретными документами и изделиями.
63. Организация допуска лиц к секретным сведениям.
64. Организация засекречивания и рассекречивания сведений.
65. Организация работы с секретными документами.
66. Защита государственной тайны.
67. Организация защиты информации в кадровой службе.
68. Организация проведения служебных расследований по фактам утраты секретных документов.
69. Защита информации при проведении совещаний и переговоров.
70. Защита информации при работе с посетителями.
71. Характеристика информационно-аналитической работы.
72. Основные направления аналитической работы на объекте защиты.
73. Этапы выполнения аналитической работы.
74. Основные методы аналитической работы.
75. Общий подход к категорированию объектов охраны.
76. Организация защита информации при публикаторской и рекламной деятельности.

77. Основные направления и методы работы с персоналом, обладающим конфиденциальной информацией.

78. Основные этапы подготовки и проведения совещаний и заседаний по конфиденциальным вопросам.

79. Лицензирование и сертификация в области защиты информации в РФ.

80. Лицензирование деятельности по защите информации.

81. Сертификация средств защиты информации

82. Коммерческая тайна и порядок её определения.

83. Организация работ с информацией, составляющей коммерческую тайну.

84. Организация и обеспечение защиты коммерческой тайны на предприятии.

85. Организация безопасности функционирования информационных систем.

86. Проведение аналитико-разведывательной работы.

87. государственная тайна и порядок отнесения к ней информации.

88. Характеристика действий по защите информации.

89. Противодействие НСД к информации.

90. Виды персональных данных в соответствии с ФЗ № 152 «О персональных данных»

91. Основные этапы создания СЗПДн на объекте.

Раздел «Инженерно-техническая защита информации»

92. Классификация информации, защищаемой техническими средствами.

93. Классификация демаскирующих признаков.

94. Принципы записи и съема информации с носителя.

95. Источники функциональных сигналов.

96. Побочные излучения и наводки. Основные понятия и классификации.

97. Характеристика основных источников информации.

98. Классификация акустоэлектрических преобразователей, создающих опасные сигналы.

99. Характеристика опасных сигналов.

100. Источники побочных высокочастотных колебании.

101. Виды паразитных связей.

102. Принципы возникновения паразитных наводок.

103. Виды угроз безопасности информации.

104. Характеристика органов добывания информации.

105. Задачи органов коммерческой разведки. Классификация видов технической разведки.

106. Характеристика видов агентурной и технической разведки.

107. Принципы добывания информации.

108. Технология добывания информации. Основные положения.

109. Основные составляющие процесса добывания информации.

110. Этапы технологии добывания информации.

111. Способы доступа к конфиденциальной информации.

112. Организация добывания информации без физического проникновения в контролируемую зону.
113. Организация доступа к источникам информации без нарушения государственной границы.
114. Особенности утечки информации по техническим каналам при эксплуатации ЭВМ.
115. Характеристики технических каналов утечки информации.
116. Структура канала передачи информации. Характеристика составляющих элементов.
117. Классификация технических каналов утечки информации.
118. Характеристика оптического КУИ.
119. Характеристика радиоэлектронного КУИ.
120. Классификация помех в технических каналах утечки.
121. Характеристика акустического КУИ.
122. Материально-вещественные каналы утечки информации.
123. Основные методы защиты информации техническими средствами.
124. Виды сокрытия информации.
125. Характеристика способов информационного сокрытия.
126. Дезинформирование. Способы. Характеристика. Основные особенности.
127. Энергетическое сокрытие.
128. Способы и средства ПДТР.
129. Способы контроля помещений на отсутствие закладных устройств.
130. Технические средства обеспечения охраны. Требования, задачи, состав.
131. Структура системы охраны объектов.
132. Способы защиты дверей и окон зданий и помещений.
133. естественные и искусственные преграды, используемые для охраны объектов.
134. Оснащение автоматизированных и автоматических контрольно-пропускных пунктов.
135. Способы и средства идентификации и аутентификации сотрудников.
136. шкафы, рабочие столы с закрываемыми на ключ ящиками, сейфы и хранилища. Виды, основные характеристики.
137. Классификация и основные элементы телевизионных систем наблюдения.
138. Компоненты и устройства ТСН.
139. Алгоритм выбора ТСН для объекта защиты.
140. Основные задачи, способы и средства инженерно-технической защиты информации.

Раздел «Программно-аппаратная защита информации»

141. Политика безопасности.
142. Матрица доступа.
143. Недостатки и достоинства схемы простой парольной аутентификации.

144. Биометрические методы идентификации и аутентификации.
145. Процедуры инициализации объекта информационной защиты.
146. Понятия идентификации и аутентификации.
147. Протоколы и алгоритмы идентификации.
148. Средства блокирования несанкционированного исследования и копирования информации КС.
149. Матричное управление доступом.
150. Функциональные блоки системы разграничения доступа к информации.
151. Функции диспетчера доступа.
152. Понятие ядра безопасности.
153. Проблемы создания высокоэффективной защиты от НСД.
154. Сравнительный анализ программных и аппаратных комплексов, рассчитанных на защиту персональных ЭВМ от несанкционированного доступа к ЭВМ, которые разграничивают доступ к информации и устройствам ПЭВМ.
155. Методы и средства обеспечения целостности и доступности информации.
156. Принципы организации защищенных систем управления.
157. Методы защиты ПК от несанкционированного доступа.
158. Группы методов защиты от угроз несанкционированного копирования.
159. Носители ключевой информации.
160. Понятие концепции иерархии ключей.
161. Распределение ключей.
162. Механизмы меток времени.
163. Методы противодействия дизассемблированию.
164. Методы противодействия трассировке программы.
165. Какие классы средств исследования программного обеспечения.
166. Функции должен выполнять инициализатора и деструктора.
167. Классификации компьютерных вирусов.
168. Группы антивирусного программного обеспечения.
169. Технологическая схема защиты.
170. Состав программного комплекса защиты.

Раздел «Криптографическая защита информации»

171. Исторические подходы к защите информации при передаче – физические методы, стенография, криптография.
172. Основные понятия и определения криптографии.
173. Классификация шифров.
174. Характер криптографической деятельности.
175. Эволюция шифров. Простейшие шифры и их свойства, композиции шифров, классические шифры, шифры гаммирования и колонной замены.
176. Алгебраические модели шифров.
177. Вероятностные модели шифров.
178. Математические модели открытых сообщений.
179. Криптографическая стойкость шифров.

180. Теоретико-информационный подход к оценке криптостойкости шифров.
181. Практическая стойкость шифров.
182. Имитостойкость шифров. Имитация и подмена сообщений.
183. Способы обеспечения имитостойости.
184. Помехостойкость шифров.
185. Практические вопросы повышения надежности.
186. Виды симметричных шифров. Особенности программной и аппаратной реализации.
187. Принцип построения блочных шифров.
188. Современные блочные криптоалгоритмы.
189. Принцип построения поточных шифров.
190. Современные поточные криптоалгоритмы.
191. Режимы использования шифров.
192. Математические основы ассиметричной криптографии.
193. Примеры современных ассиметричных шифров.
194. Криптографические хэш-функции.
195. Задачи и особенности электронно-цифровой подписи.
196. Алгоритм цифровой подписи.
197. Симметричные (одноразовые) цифровые подписи.
198. Протокол распределения ключей.
199. Передача ключей с использованием симметричного и ассиметричного шифрования.
200. Открытое и предварительное распределение ключей.
201. Схемы распределения секрета.
202. Методы применения шифрования данных в локальных вычислительных сетях.
203. Обеспечение секретности данных при долгосрочном хранении
204. Задачи обеспечения секретности и целостности данных и ключей при краткосрочном хранении
205. Обеспечение секретности ключей при долгосрочном хранении
206. Защита от атак с использованием побочных каналов
207. Эллиптические кривые
208. Квантовая криптография

Раздел «Защита персональных данных»

209. Европейская конвенция о защите физических лиц при автоматизированной обработке персональных данных.
210. Методика определения актуальных угроз безопасности ИСПДн.
211. ФЗ № 152 «О персональных данных».
212. Модель угроз безопасности ИСПДн.
213. Постановление № 1119 « Об утверждении порядка требований к защите персональных данных при их обработке в информационных системах персональных данных».
214. Модель нарушителя.

215. Обеспечение контроля и надзора за выполнением требований по защите ПДн. Виды предусмотренных законодательством проверок.

216. Определения уровня защищенности ИСПДн

217. Типы информационных систем персональных данных

218. Виды программно-аппаратных средств защиты ИСПДн (примеры).

219. .Порядок определения наличия недекларированных возможностей в системной и прикладном ПО

220. Перечень организационно-распорядительных документов, регламентирующих защиту ПДн и ИСПДн на объекте.

221. Виды технических средств защиты ИСПДн (примеры).

222. Перечень нормативно-правовых актов, регламентирующих порядок наказаний за нарушение правил обработки персональных данных.

223. Выполнение мер по защите информационных систем персональных данных в соответствии с приказом № 21 ФСТЭК «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

224. Модель угроз безопасности ИСПДн.

225. Перечень мер по защите ПДн, обрабатываемых без использования средств автоматизации.

Раздел «Управление интеллектуальной собственностью»

226. Понятие «интеллектуальная собственность»

227. Основные институты права интеллектуальной собственности;

228. Объекты интеллектуальной собственности, авторское право;

229. Особенности защиты служебной и коммерческой информации;

230. Общие признаки объектов интеллектуальной собственности;

231. Права авторов и патентообладателей интеллектуальной собственности;

232. Система правовой охраны интеллектуальной собственности;

233. Правовая охрана служебной и коммерческой тайны;

234. Институт права средств индивидуализации;

235. Международная патентная классификация, её структура;

236. Основные разделы патентного закона Российской Федерации;

237. Всемирная организация интеллектуальной собственности;

238. Гражданско-правовые способы защиты прав авторов и патентообладателей;

239. Международное сотрудничество в области промышленной собственности;

240. Право преждепользования, права патентообладателей.