Приложение
05.13.19 Методы и системы защиты информации, информационная безопасность

ПРОГРАММА КАНДИДАТСКОГО ЭКЗАМЕНА
Приложение к рабочей программе по дисциплине Методы и системы защиты информации, информационная безопасность, направленной на подготовку к сдаче кандидатских экзаменов

1. Общие положения

Кандидатские экзамены являются составной частью аттестации научных и научно-педагогических кадров. Цель экзамена - установить глубину профессиональных знаний аспиранта, уровень подготовленности к самостоятельной научно-исследовательской работе.

Сдача кандидатских экзаменов обязательна для присуждения ученой степени кандидата наук, а также для соискателей ученой степени доктора наук, не имеющих ученой степени кандидата наук.

Во время сдачи кандидатского экзамена по специальной дисциплине аспирант должен продемонстрировать глубокие знания теоретических основ избранного научного направления, понимать ее проблематику, ориентироваться в применяемых методиках.

Кандидатский экзамен по специальности состоит из двух частей:

1. Ответ на экзаменационные вопросы по специальности.
2. Защита реферата, тема которого отвечает проблематике специальности. Реферат сдается не менее чем за 10 дней до экзамена научному руководителю аспиранта.

Кандидатский экзамен по специальности сдается на четвертом году обучения в аспирантуре.

Настоящая программа кандидатского экзамена по научной специальности 05.13.19 Методы и системы защиты информации, информационная безопасность, составлена в соответствии с федеральным государственным образовательным стандартом высшего профессионального образования и разработана согласно требованиям законодательства Российской Федерации в системе послевузовского профессионального образования.

Она охватывает область науки и техники, в рамках которой разрабатываются теории, системы, модели, методы, а также программные, аппаратно-программные, технические средства защиты информации и оценка ее защищенности в процессе сбора, хранения, обработки, передачи и распространения с использованием информационных технологий; исследуются научно-технические аспекты информационной безопасности объектов информационной сферы. В основу программы положены следующие дисциплины: основы информационной безопасности, технические средства и методы защиты информации, криптографические

методы защиты информации, программно-аппаратные средства обеспечения информационной безопасности, защита от разрушающих программных воздействий.

Дополнительно к основной программе каждым аспирантом по теме диссертационного исследования готовятся дополнительные вопросы.

Цель программы - проверка соответствия подготовки аспирантов требованиям современного уровня науки и практики в области защиты информации и информационной безопасности по специальности 05.13.19.

Требования к уровню знаний аспиранта. Аспиранты должны знать:

- термины и определения методов и систем защиты информации и информационной безопасности;
- принципы построения современных систем и средств защиты информации;
- основные положения, методы и системы обеспечения безопасности информационных систем (СВТ, АС);
- методы и системы защиты, оценки защищенности и принятых мер защиты информации, методологию создания защищенных информационных систем;
- основы криптографических и инженерно-криптографических методов, предотвращающих или существенно затрудняющих несанкционированный доступ (НСД) к информации;
- методы и средства защиты информации от утечки по техническим каналам (СВТ, АС, ТСПИ и ВТСС);
- основы теории кодирования;
- основы теории технической защиты информации;
- основы информационной безопасности;
- теорию вероятностей, математическую статистику, теорию информации;
- архитектуру вычислительных систем (СВТ, АС) и сетей;
- технологии программирования на языках высокого и низкого уровней.

Разделы программы охватывают следующие направления:

- методологию создания и оценку защищенности информационных систем;
- основные направления развития программно-аппаратных систем защиты информации и оценки ее защищенности;
- администрирование и политику безопасности защиты информации вычислительных систем и сетей;
- правовое обеспечение защиты информации;
- организацию взаимодействия абонентов информационных систем с помощью криптографических протоколов;
- принципы построения и методы криптоанализа современных блочных и поточных криптосистем;

- стеганографию и другие методы защиты и безопасности информации.

Процедура приема кандидатских экзаменов регламентирована Положением о подготовке научно-педагогических и научных кадров в системе послевузовского профессионального образования в Российской Федерации, утвержденного приказом Министерства общего и профессионального образования РФ от 27.03.1998 № 814 (в действующей редакции).

Результаты экзамена оцениваются как «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Пересдача кандидатского экзамена не допускается. Результаты кандидатских экзаменов действительны до срока действия номенклатуры специальностей.

2. Цель кандидатского экзамена

Целью кандидатского экзамена по научной специальности «Методы и системы защиты информации, информационная безопасность» является определение уровня знаний, полученных аспирантами в результате освоения образовательных программ высшего образования, их готовность к защите кандидатской диссертации.

3. Содержание программы

Раздел 1. Модели и методы формирования требований и оценки безопасности систем информационных технологий

Законодательные и правовые основы защиты компьютерной информации информационных технологий. Безопасность информационных ресурсов и документирование информации. Государственные информационные ресурсы, персональные данные о гражданах, права на доступ к информации, разработка и производство информационных систем, вычислительные сети и защита информации. Нормативно-правовая база функционирования систем защиты информации. Компьютерные преступления и особенности их расследования. Российское законодательство по защите информационных технологий. Промышленный шпионаж и законодательство, правовая защита программного обеспечения авторским правом.

Информационная безопасность. Критерии оценки безопасности информационных технологий. Стандарты серии СТБ 11.34.101 (ИСО/МЭК 15408). Профиль защиты и задание по обеспечению безопасности. Угрозы, политика и задачи безопасности. Функциональные и гарантийные требования безопасности.

Политика безопасности. Модель Белла – Лападула. Модель take-grant. Дискреционная политика. Ролевая политика. Мандатная политика. Политика контроля целостности. Модель Биба. Модель Кларка – Вилсона.

Административный уровень обеспечения безопасности информационных систем. Стандарт ISO/IEC 17799. Организационные меры

по обеспечению безопасности. Управление ресурсами. Безопасность персонала. Физическая безопасность. Управление коммуникациями и процессами. Контроль доступа. Программные средства.

Экономические аспекты безопасности информационных систем. Методические рекомендации по проведению экспертизы при оценке систем защиты информации. Применение программных средств для расчета стоимости внедрения системы безопасности.

Раздел 2. Модели защиты и методы для формирования требований и оценки безопасности программных и аппаратно-программных средств защиты информации и организационных мер защиты от НСД

Анализ угроз информационной безопасности. Проблемы информационной защиты. Классификация угроз информационной безопасности. Виды представления информации и возможные каналы утечки. Модель вероятного нарушителя. Виды, источники и носители защищаемой информации. Основные каналы утечки информации. Побочные электромагнитные излучения и наводки. Техническое вооружение нарушителя.

Аппаратное и программное обеспечение комплексной информационной защиты (реализация требований к защите от НСД к информации, от утечки по техническим каналам, от возможного внедренного специальных электронных устройств и программного обеспечения). Типы и виды аппаратуры формирования, обработки, передачи и хранения конфиденциальных данных. Обеспечение программно-технических мер по предотвращению утечки информации. Реализация требований по информационной защите и оценке принятых мер защиты от утечки по техническим каналам. Защита от ПЭМИН СВТ, АС, ТСПИ, ВТСС.

Комплекс организационных мер и программно-технических (в том числе криптографических современных методов и средств защиты информации, защиты от утечки за счет побочного электромагнитных, акустического и виброакустического, оптического и других излучений и наводок) средств обеспечения безопасности информации в АС и СВТ от внутренних и внешних угроз.

Обеспечение сетевой безопасности. Защита от НСД в глобальных и локальных сетях. Межсетевые фильтры и брандмауэры, firewall. Реализация защиты данных на канальном уровне. Реализация протоколов безопасной электронной почты.

Реализация криптографических алгоритмов и протоколов. Высокопроизводительные программируемые безопасные процессоры и сопроцессоры, программируемые логические интегральные схемы. Быстродействующая гибкая архитектура для обеспечения секретных коммуникаций.

Специализированные аппаратно-программные средства обеспечения информационной безопасности. Устройства управления доступом. Электронные ключи iButton. Смарт-карты. Специализированные

встраиваемые платы. Спецпроцессоры, контроллеры и программно-перестраиваемые модули. Эмуляторы и симуляторы. Построение генераторов случайных чисел на физическом источнике. Настройка и оценка качества. Специализированные статистические тесты. Модемы для обеспечения конфиденциальных транзакций.

Программные и аппаратно-программные средства защиты информации от копирования и взлома. Верификация.

Активные и пассивные методы информационной защиты каналов утечки информации. Основные характеристики технических средств защиты от утечки информации по техническим каналам.

Раздел 3. Математические модели, методы и алгоритмы анализа и синтеза криптографических преобразований информации

История криптографии. Задачи криптографии и криптоанализа. Криптосистемы (шифрсистемы). Шифры перестановки, замены, Виженера, Вернама. Элементы теории Шеннона. Совершенные криптосистемы. Расстояние единственности.

Блочные криптосистемы. Схема подстановки-перестановки. Схема Фейстеля. Режимы шифрования (простой замены, счетчика, цепной обработки, гаммирования с обратной связью). Блочные криптосистемы DES, ГОСТ 28147-89, AES.

Криптоаналитические атаки. Условия проведения атак. Задачи криптоанализа. Сложность атак. Криптоанализ «грубой силой». Баланс «время – память». Разностный криптоанализ. Линейный криптоанализ.

Поточные криптосистемы. Конечные автоматы. Регистры сдвига с линейной обратной связью. Фильтрующий генератор. Комбинирующий генератор. Генератор с неравномерным движением. Сжимающий и самосжимающий генератор. Линейная сложность. Корреляционный криптоанализ. Поточная криптосистема A5/1.

Функции хэширования. Блочно-итерационные функции хэширования. Атака «дней рождения». Ключезависимые функции хэширования. Генераторы псевдослучайных чисел на основе функций хэширования. Функция хэширования СТБ 1176.1-99.

Функции «с лазейкой». Использование функций «с лазейкой» для построения криптосистем с открытым ключом. Функция Рабина. Функция RSA. RSA и факторизация. Электронная цифровая подпись. Схема Эль-Гамаля. Схема Шнорра. Система ЭЦП СТБ 1176.2.

Раздел 4. Модели, методы и алгоритмы анализа и синтеза криптографических протоколов

Определение, назначение, область применения криптографических протоколов. Типы ключей и их взаимосвязи. Генерация и распределение ключей. Разновидности атак на протоколы.

Протоколы аутентификации. Протоколы, основанные на симметричном алгоритме шифрования и MAC-коде. Стандарты ISO/IEC 9798-2, 4.

Протоколы распределения ключей. Протоколы без участия третьей доверенной стороны. Протоколы с участием третьей доверенной стороны. Стандарты ISO/IEC 9798-2, ISO/IEC 11770-2. Использование асимметричных криптосистем: протокол Диффи – Хеллмана, протокол Нидхема – Шредера. Практические криптографические протоколы. Протоколы NTLM, Kerberos, SSL, IPSec.

Управление ключами. Жизненный цикл ключей. Инфраструктура открытых ключей. Структура сертификата и списка отозванных сертификатов X.509. Форматы данных PKCS#7 аппаратного и программного обеспечения. Противодействие исследованию программ. Обфускация программ.

Раздел 5. Методы, системы, средства защиты информации, основанные на стеганографии, квантовой криптографии

Квантовая криптография. Квантовые эффекты, используемые для создания канала передачи ключевой информации. Протокол Беннета – Брассара. Устранение ошибок. Практическая реализуемость квантовой передачи ключей. Стеганография. Структурная схема и математическая модель типовой стеганосистемы. Протоколы стеганографических систем. Бесключевые, с открытым ключом, смешанные системы.

Принципы стеганографического анализа. Виды атак на стенографическую систему. Основные этапы практического стеганоанализа. Оценка качества стеганосистем. Абсолютно надежная стеганосистема. Пропускная способность каналов передачи скрываемых данных. Информационное скрытие при активном противодействии. Свойства скрытой пропускной способности стеганоканала.

Скрытие данных в неподвижных изображениях. Обзор стегоалгоритмов встраивания информации в изображения. Скрытие данных в видеопоследовательностях. Краткое описание стандарта MPEG и возможности внедрения данных. Скрытие данных в аудиосигналах. Оценка стойкости стеганографических систем. Цифровые водяные знаки.

4. Перечень примерных вопросов

1. Законодательные и правовые основы защиты компьютерной информации информационных технологий. Безопасность информационных ресурсов и документирование информации; государственные информационные ресурсы; персональные данные о гражданах; права на доступ к информации;

2. Вычислительные сети и защита информации; нормативно-правовая база функционирования систем защиты информации; компьютерные преступления и особенности их расследования; российское законодательство по защите информационных технологий; промышленный шпионаж и законодательство, правовая защита программного обеспечения авторским правом.

3. Информационная безопасность. Критерии оценки безопасности информационных технологий. Стандарты серии СТБ 11.34.101 (ИСО/МЭК 15408). Профиль защиты и задание по обеспечению безопасности. Угрозы, политика и задачи безопасности. Функциональные и гарантийные требования безопасности.

4. Административный уровень обеспечения безопасности информационных систем. Стандарт ISO/IEC 17799. Организационные меры по обеспечению безопасности. Управление ресурсами. Безопасность персонала. Физическая безопасность. Управление коммуникациями и процессами. Контроль доступа. Программные средства.

5. Анализ угроз информационной безопасности. Проблемы информационной защиты. Классификация угроз информационной безопасности. Виды представления информации и возможные каналы утечки. Модель вероятного нарушителя. Виды, источники и носители защищаемой информации.

6. Аппаратное и программное обеспечение комплексной информационной защиты. Типы и виды аппаратуры формирования, обработки, передачи и хранения конфиденциальных данных. Обеспечение программно-технических мер по предотвращению утечки информации.

7. Комплекс организационных мер и программно-технических средств обеспечения безопасности информации в АС и СВТ от внутренних и внешних угроз.

8. Обеспечение сетевой безопасности. Защита от НСД в глобальных и локальных сетях. Межсетевые фильтры и брандмауэры, firewall. Реализация защиты данных на канальном уровне. Реализация протоколов безопасной электронной почты.

9. Реализация криптографических алгоритмов и протоколов. Высокопроизводительные программируемые безопасные процессоры и сопроцессоры, программируемые логические интегральные схемы. Быстродействующая гибкая архитектура для обеспечения секретных коммуникаций.

10. Специализированные аппаратно-программные средства обеспечения информационной безопасности. Устройства управления доступом. Электронные ключи iButton. Смарт-карты. Специализированные встраиваемые платы. Спецпроцессоры, контроллеры и программно-перестраиваемые модули. Эмуляторы и симуляторы. Модемы для обеспечения конфиденциальных транзакций.

11. Программные и аппаратно-программные средства защиты информации от копирования и взлома. Верификация.

12. Активные и пассивные методы информационной защиты каналов утечки информации. Основные характеристики технических средств защиты от утечки информации по техническим каналам.

13. История криптографии. Задачи криптографии и криптоанализа. Криптосистемы (шифрсистемы). Шифры перестановки, замены, Виженера, Вернама. Элементы теории Шеннона. Совершенные криптосистемы.

14. Криптоаналитические атаки. Условия проведения атак. Задачи криптоанализа. Сложность атак. Криптоанализ «грубой силой». Баланс «время – память». Разностный криптоанализ. Линейный криптоанализ.

15. Поточные криптосистемы. Конечные автоматы. Регистры сдвига с линейной обратной связью. Фильтрующий генератор. Комбинирующий генератор. Генератор с неравномерным движением. Сжимающий и самосжимающий генератор. Линейная сложность. Корреляционный криптоанализ. Поточная криптосистема A5/1.

16. Функции хэширования. Блочно-итерационные функции хэширования. Атака «дней рождения». Ключезависимые функции хэширования. Генераторы псевдослучайных чисел на основе функций хэширования. Функция хэширования СТБ 1176.1-99.

17. Определение, назначение, область применения криптографических протоколов. Типы ключей и их взаимосвязи. Генерация и распределение ключей. Разновидности атак на протоколы.

18. Протоколы аутентификации. Протоколы, основанные на симметричном алгоритме шифрования и MAC-коде. Протоколы распределения ключей. Протоколы без участия третьей доверенной стороны. Протоколы с участием третьей доверенной стороны.

19. Управление ключами. Жизненный цикл ключей. Инфраструктура открытых ключей. Структура сертификата и списка отозванных сертификатов X.509. Форматы данных PKCS#7 аппаратного и программного обеспечения. Противодействие исследованию программ. Обфускация программ.

20. Квантовая криптография. Квантовые эффекты, используемые для создания канала передачи ключевой информации. Протокол Беннета – Брассара. Устранение ошибок. Практическая реализуемость квантовой передачи ключей. Стеганография. Структурная схема и математическая модель типовой стеганосистемы. Протоколы стеганографических систем. Бесключевые, с открытым ключом, смешанные системы.

21. Принципы стеганографического анализа. Виды атак на стенографическую систему. Основные этапы практического стеганоанализа. Оценка качества стеганосистем. Абсолютно надежная стеганосистема. Пропускная способность каналов передачи скрываемых данных. Информационное скрытие при активном противодействии. Свойства скрытой пропускной способности стеганоканала.

22. Скрытие данных в неподвижных изображениях. Обзор стегоалгоритмов встраивания информации в изображения. Скрытие данных в видеопоследовательностях. Краткое описание стандарта MPEG и возможности внедрения данных. Скрытие данных в аудиосигналах.