МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования

«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ» (ТУСУР)

ПОСЛЕВУЗОВСКОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАНИЕ (АСПИРАНТУРА)

УТВЕРЖДАЮ
Проректор по научной работе
_____ Шелупанов А.А.
«___»_____2012 г.

ПРОГРАММА

Кандидатского экзамена

по специальности

05.13.19 - МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

КЭ А.03; цикл «Кандидатские экзамены» основной образовательной программы подготовки аспиранта по отрасли 05.00.00 – технические науки,

Присуждаемая ученая степень:	кандидат наук
Форма обучения:	очная/заочная
Руководитель ООП:	Шелупанов А.А., д.т.н., профессор

Томск 2012 г.

Программа кандидатских экзаменов составлена на основании:

Федеральных государственных требований к структуре основной профессиональной образовательной программы послевузовского профессионального образования (аспирантура), утвержденных приказом Минобрнауки России от 16.03.2011 № 1365;

Паспорта научной специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность;

Программы – минимум кандидатского экзамена по научной специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

В соответствии с учебными планами очной/заочной формы обучения, утвержденными решением Ученого совета университета «27» июня 2012, протокол № 6.

Составители рабочей программы: Шелупанов А.А., д.т.н., профессор, зав. кафедрой комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС); Мещеряков Р.В., д.т.н., доцент кафедры КИБЭВС.

РАБОЧАЯ ПРОГРАММА РАССМОТРЕНА И ОДОБРЕНА на заседании обеспечивающей кафедры КИБЭВС протокол № ____ от _____2012 г.

Научный руководитель программы
аспирантской подготовки А.А. Шелупанов

СОГЛАСОВАНО:

Зав. ОППО И.А. Ярымова

Декан ФВС М.В. Черкашин

Зав. обеспечивающей кафедры КИБЭВС А.А. Шелупанов

Разработчик Р.В. Мещеряков

ОБЩИЕ ПОЛОЖЕНИЯ

Кандидатский экзамен по специальной дисциплине в соответствии с темой диссертации КЭ.А.03 относится к циклу КЭ.А.ОО – кандидатские экзамены и входит в состав исследовательской составляющей учебного плана подготовки аспирантов.

Кандидатский экзамен по специальной дисциплине в соответствии с темой диссертации КЭ.А.03 является формой отчетности по специальной дисциплине ОДА.03 « Методы и системы защиты информации, информационная безопасность» и научной специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность и дисциплинам ОДА.04 по выбору аспиранта «Основы информационной безопасности», «Правовое обеспечение информационной безопасности», «Организационное обеспечение информационной безопасности»

Предметом кандидатского экзамена по специальной дисциплине в соответствии с темой диссертации являются знания, умения и владения научной специальностью 05.13.19 – Методы и системы защиты информации, информационная безопасность в соответствии с формулой специальности:

Методы и системы защиты информации, информационная безопасность – специальность, включающая исследования проблем разработки, совершенствования и применения методов и средств защиты информации в процессе ее сбора, хранения, обработки, передачи и распространения, а также обеспечения информационной безопасности объектов политической, социально-экономической, оборонной, культурной и других сфер деятельности от внешних и внутренних угроз хищения, разрушения и/или модификации информации.

Значение решения научных и технических проблем данной специальности для народного хозяйства состоит в разработке новых и совершенствовании имеющихся методов и средств защиты информации и обеспечения информационной безопасности.

А также областями исследований:

1. Теория и методология обеспечения информационной безопасности и защиты информации.
2. Методы, аппаратно-программные и организационные средства защиты систем (объектов) формирования и предоставления пользователям информационных ресурсов различного вида.
3. Методы, модели и средства выявления, идентификации и классификации угроз нарушения информационной безопасности объектов различного вида и класса.
4. Системы документооборота (вне зависимости от степени их компьютеризации) и средства зашиты циркулирующей в них информации.
5. Методы и средства (комплексы средств) информационного противодействия угрозам нарушения информационной безопасности в открытых компьютерных сетях, включая Интернет.
6. Модели и методы формирования комплексов средств противодействия угрозам хищения (разрушения, модификации) информации и нарушения информационной безопасности для различного вида объектов защиты вне зависимости от области их функционирования.
7. Анализ рисков нарушения информационной безопасности и уязвимости процессов переработки информации в информационных системах любого вида и области применения.
8. Модели противодействия угрозам нарушения информационной безопасности для любого вида информационных систем.
9. Модели и методы оценки защищенности информации и информационной безопасности объекта.
10. Модели и методы оценки эффективности систем (комплексов) обеспечения информационной безопасности объектов защиты.

11. Технологии идентификации и аутентификации пользователей и субъектов информационных процессов. Системы разграничения доступа.
12. Мероприятия и механизмы формирования политики обеспечения информационной безопасности для объектов всех уровней иерархии системы управления.
13. Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности.
14. Модели, методы и средства обеспечения внутреннего аудита и мониторинга состояния объекта, находящегося под воздействием угроз нарушения его информационной безопасности.
15. Модели и методы управления информационной безопасностью.

Программа кандидатского экзамена по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность предназначена для аспирантов (соискателей степени кандидата наук) в качестве руководящего учебно-методического документа для целенаправленной подготовки к сдаче кандидатского экзамена.

Цель экзамена - установить глубину профессиональных знаний соискателя ученой степени, уровень подготовленности к самостоятельной научно-исследовательской работе. Сдача кандидатского экзамена по специальности обязательна для присуждения ученой степени кандидата наук.

Кандидатский экзамен по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность сдается в сроки, определенные учебным планом специальности.

Для проведения экзамена приказом ректора (проректора по науке) создается экзаменационная комиссия, которая формируется из высококвалифицированных научно-педагогических и научных кадров, включая научных руководителей аспирантов. Комиссия правомочна принимать кандидатский экзамен, если в ее заседании участвуют не менее двух специалистов по профилю принимаемого экзамена, в том числе один доктор наук. При приеме экзамена могут присутствовать члены соответствующего диссертационного совета организации, где принимается экзамен, ректор, проректор, декан, представители министерства или ведомства, которому подчинена организация.

Во время проведения экзамена соискателю ученой степени задаются вопросы по основной и дополнительной программам.

Кандидатский экзамен проводится по усмотрению экзаменационной комиссии по билетам или без билетов. Для подготовки ответа аспирант (соискатель ученой степени) использует экзаменационные листы, которые сохраняются после приема экзамена в течение года по месту сдачи экзамена.

На каждого соискателя ученой степени заполняется протокол приема кандидатского экзамена, в который вносятся вопросы билетов и вопросы, заданные соискателю членами комиссии.

Уровень знаний соискателя ученой степени оценивается на «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Протокол приема кандидатского экзамена подписывается членами комиссии с указанием их ученой степени, ученого звания, занимаемой должности и специальности согласно номенклатуре специальностей научных работников.

Протоколы заседаний экзаменационных комиссий после утверждения ректором (проректором по научной работе) ТУСУРа хранятся в отделе аспирантуры и докторантуры. О сдаче кандидатского экзамена выдается удостоверение установленной формы.

СОДЕРЖАНИЕ ПРОГРАММЫ

I ЧАСТЬ. ПРОГРАММА-МИНИМУМ

кандидатского экзамена по специальности

05.13.19 – Методы и системы защиты информации, информационная безопасность по техническим наукам

Введение

В основу настоящей 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.

1. Методы и системы защиты информации

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.

Проблемы защиты информации в информационных системах. Меры по обеспечению сохранности информации и угрозы ее безопасности в информационных системах; основные задачи обеспечения безопасности информации в информационных системах; защита локальных сетей и операционных систем; интеграция систем защиты; Internet в структуре информационно-аналитического обеспечения информационных систем; рекомендации по защите информации в Internet.

Содержание системы средств защиты компьютерной информации в информационных системах. Защищенная информационная система и система защиты информации; принципы построения систем защиты информации и их основы; законодательная, нормативно-методическая и научная база системы защиты информации.

Требования к содержанию нормативно-методических документов по защите информации; научно-методологический базис, стратегическая направленность и инструментальный базис защиты информации; структура и задачи (типовой перечень) органов, выполняющих защиту информации.

Организационно-правовой статус службы информационной безопасности; организационно-технические и режимные меры; политика безопасности: организация секретного делопроизводства и мероприятий по защите информации; программно-технические методы и средства защиты информации; программно-аппаратные методы и средства ограничения доступа к компонентам компьютера; типы несанкционированного доступа и условия работы средств защиты; вариант защиты от локального несанкционированного доступа и от удаленного ИСД.

Средства защиты, управляемые модемом, надежность средств защиты.

2 . Информационная безопасность

Изучение традиционных симметричных криптосистем. Основные понятия и определения; шифры перестановки; шифр перестановки «скитала»; шифрующие таблицы; применение магических квадратов; шифры простой замены; полибианский квадрат; система шифрования Цезаря; система шифрования Вижинера; шифр «двойной квадрат» Уитстона; одноразовая система шифрования; шифрование методом Вернама; роторные машины; шифрование методом гаммирования; методы генерации псевдослучайных последовательностей чисел.

Применение симметричных криптосистем для защиты компьютерной информации в информационных системах. Изучение американского стандарта шифрования данных DES; основные режимы работы алгоритма DES; отечественный стандарт шифрования данных; режим простой замены; режим гаммирования; режим гаммирования с обратной связью; режим выработки имитовставки; блочные и поточные шифры.

Применение асимметричных криптосистем для защиты компьютерной информации в информационных ситемах. Концепция криптосистемы с открытым ключом; однонаправленные функции; криптосистема шифровывания данных RSA (процедуры шифрования и расшифрования в этой системе); безопасность и быстродействие криптосистемы RSA; схема шифрования Полига—Хеллмана; схема шифрования эль-Гамаля, комбинированный метод шифрования.

Методы идентификации и проверки подлинности пользователей компьютерных систем. Основные понятия и концепции; идентификация и механизмы подтверждения подлинности пользователя; взаимная проверка подлинности пользователей; протоколы идентификации с нулевой передачей знаний; упрощенная схема идентификации с нулевой передачей знаний; проблема аутентификации данных и электронная цифровая подпись; однонаправленные хэш-функции; алгоритм безопасного деширования SHA; однонаправленные хэш-функции на основе симметричных блочных алгоритмов; отечественный стандарт хэш-функции; алгоритм цифровой подписи RSA; алгоритм цифровой подписи эль-Гамаля (EGSA); алгоритм цифровой подписи DSA; отечественный стандарт цифровой подписи.

Защита компьютерных систем от удаленных атак через сеть Internet

Режим функционирования межсетевых экранов и их основные компоненты; маршрутизаторы; шлюзы сетевого уровня; усиленная аутентификация; основные схемы сетевой защиты на базе межсетевых экранов; применение межсетевых экранов для организации виртуальных корпоративных сетей; программные методы защиты.

Изучение существующих аппаратно-программных средств криптографической защиты компьютерной информации серии КРИПТОН. Основные элементы средств защиты сети от несанкционированного доступа; устройства криптографической защиты данных; контроллер смарт-карт SCAT-200; программно-аппаратная система защиты от несанкционированного доступа (НСД) КРИПТОН-ВЕТО; защита от НСД со стороны сети; абонентское шифрование и ЭЦП; шифрование пакетов; аутентификация; защита компонентов ЛВС от НСД; защита абонентского пункта, маршрутизаторов и устройств контроля; технология работы с ключами.

Методы защиты программ от изучения и разрушающих программных воздействий (программных закладок и вирусов). Классификация способов защиты; защита от отладок и дизассемблирования; способы встраивания защитных механизмов в программное обеспечение; понятие разрушающего программного воздействия; модели взаимодействия прикладной программы и программной закладки; методы перехвата и навязывания информации; методы внедрения программных закладок; компьютерные вирусы как особый класс разрушающих программных воздействий; защита от РПВ; понятие изолированной программной среды.

Комплексная защита процесса обработки информации в компьютерных системах на основе стохастической интеллектуальной информационной технологии. Возможности СИИТ для обеспечения комплексной защиты программ в момент их выполнения и данных при их обработке в компьютере; метод верификации программного обеспечения для контроля корректности, реализуемости и защиты от закладок.

Разработка транслятора исходного текста программ, обеспечивающего их защиту на логическом (алгоритмическом) и физическом уровне от НСД, программных закладок и вирусов.

Метод защиты от НСД и разрушающих программных воздействий процесса хранения, обработки информации; защита арифметических вычислений в компьютерных системах; основные направления создания защищенных компьютерных систем нового поколения на основе СИИТ.

II ЧАСТЬ. ДОПОЛНИТЕЛЬНАЯ ПРОГРАММА

кандидатского экзамена по специальности

05.13.19 – Методы и системы защиты информации, информационная безопасность

Для каждого диссертанта предлагается своя программа-максимум кандидатского экзамена по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность в соответствии с его темой кандидатской диссертации и является дополнением к программе-минимум кандидатского экзамена по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

Индивидуальная Дополнительная программа разрабатывается научным руководителем соискателя и кафедрой (лабораторией, центром, институтом) на основании диссертационного исследования соискателя и должна быть представлена в отдел аспирантуры не менее, чем за 2 недели до даты сдачи кандидатского экзамена.

В дополнительной программе должны быть отражены последние научные достижения в области науки, в рамках которой проведено диссертационное исследование, использована новейшая научная отечественная и зарубежная литература, интернет-издания, а также справочно-информационные издания соответствующей тематики. Дополнительная программа должна соответствовать требованиям, предъявляемым к дополнительным программам в ТУСУРе.

Дополнительная программа обсуждается на заседании кафедры (лаборатории, центра, института) ТУСУРа, на которой разработана программа и выносится для утверждения на заседание Совета факультета.

Для соискателей ученой степени, не являющихся сотрудниками или аспирантами ТУСУРа, дополнительная программа обсуждается на заседании кафедры (лаборатории, центра, института) ТУСУРа, на которой ведется подготовка аспирантов по соответствующей научной специальности, и выносится для утверждения на заседание Совета факультета.

Дополнительная программа утверждается Советом факультета не менее, чем за 1 месяц до даты проведения кандидатского экзамена.

УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

Основная литература

1. Программно-аппаратные средства обеспечения информационной безопасности : учебное пособие: В 2 разделах / А. П. Зайцев; Министерство образования и науки Российской Федерации, Томский государственный университет систем управления и радиоэлектроники, Кафедра комплексной информационной безопасности электронно-вычислительных систем. - Томск : В-Спектр, 2007 - . (66 экз.).

2. Основы защиты информации: Учебное пособие/ сост.: А. А. Шелупанов [и др.]. - Томск: В-Спектр, 2011. - 151 с.: ил. Электронный ресурс. (http://kibevs.tusur.ru/sites/default/files/upload/manuals/shelupanov_ozi.pdf).

Дополнительная литература

1. Информационная безопасность и защита информации: Учебное пособие для вузов / В. П. Мельников, С. А. Клейменов, А. М. Петраков; ред.: С. А. Клейменов. - М.: Academia, 2006. - 330[6] с.: граф., ил., табл. - (Высшее профессиональное образование. Информатика и вычислительная техника). - Библиогр.: с. 327-328. - ISBN 5-7695-2592-4. (30 экз.)

2. Основы информационной безопасности: Учебное пособие для вузов / Е. Б. Белов [и др.]. - М.: Горячая линия-Телеком, 2006. - 544 с.: табл. - (Учебное пособие) (Специальность для высших учебных заведений). - ISBN 5-93517-292-5: 200.00 р., 209.99 р. (80 экз.)

3. Основы информационной безопасности: учебное пособие для вузов/ В. А. Галатенко; ред. В. Б. Бетелин. - 4-е изд. - М.: Интернет-Университет Информационных Технологий, 2008; М.: БИНОМ. Лаборатория знаний, 2008. - 205[3] с. (1 экз.)

4. Информационная безопасность открытых систем: В 2 т.: Учебник для вузов. Том 1./ С. В. Запечников [и др.]. - М.: Горячая линия-Телеком, 2006. (10 экз.)

5. Системный анализ в защите информации: Учебное пособие для вузов/ А. А. Шумский, А. А. Шелупанов. - М.: Гелиос АРВ, 2005. - 220 с. (33 экз.)

Периодические издания

Вопросы защиты информации
Информатика и системы управления
Доклады ТУСУР
Труды СПИИРАН
Информация и безопасность
Компьютерные системы: информационная безопасность

Перечень интернет-ресурсов

www.elibrary.ru
www.algoritms.ru
www.intuit.ru
сайты журналов