МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное
учреждение высшего профессионального образования
«Пензенский государственный университет»
(ФГБОУ ВПО «Пензенский государственный университет»)

ПРОГРАММА
кандидатского экзамена по специальности

05.13.19 «Методы и системы защиты информации. Информационная безопасность» (по техническим наукам)

для аспирантов и соискателей кафедры ИБСТ

Утверждена
На заседании Ученого Совета ПГУ

Протокол № 1 от 18.09 2014 г.

Председатель Ученого Совета ПГУ
Ректор ПГУ

_____ А.Д. Гуляков

ПРОГРАММА
кандидатского экзамена по специальности
05.13.19 «Методы и системы защиты информации. Информационная безопасность»
(по техническим наукам)

1 Основы теории защиты информации

Особенности информатизации общества на современном этапе. Основные характеристики современных информационных систем. Необходимость обеспечения информационной безопасности систем и объектов.

Возникновение проблемы защиты информации. Развитие и становление способов защиты. Этапы развития и их характеристики.

Определение, особенности и общее содержание теории защиты информации.

Научно-методологический базис теории защиты. Система моделей защиты информации.

Определение и основные понятия стратегии защиты информации. Факторы, влияющие на формирование стратегий защиты. Классификационная структура множества необходимых стратегий защиты. Общая характеристика основных стратегий.

Определение и назначение инструментально-методологического базиса защиты информации. Требования к инструментально-методологическому базису.

Пути и способы реализации основных положений теории защиты информации.

Перспективы и проблемы развития теории и практики защиты.

2 Угрозы информации и методология оценки ее уязвимости

Определение и природа угроз информации в современных системах ее обработки.

Классификация и общая характеристика основных угроз.

Понятие уязвимости информации. Подходы к определению значений показателей уязвимости.

Эмпирические методы определения значений показателей уязвимости. Примеры эмпирических моделей. Способы определения параметров моделей. Особенности использования моделей.

Теоретико-вероятностные методы определения значений показателей уязвимости, подходы к построению моделей. Примеры моделей. Особенности и проблемы практического использования.

Теоретико-эмпирические методы определения значений показателей. Подходы к построению теоретико-эмпирических моделей. Понятие базового показателя уязвимости, аналитическая и статистическая модели его определения.

Методы и модели прогнозирования значений показателей уязвимости.

Определение, значение, структура и способы формирования инструментальных средств оценки уязвимости информации.

3 Методы обеспечения информационной безопасности

Защита автоматизированных 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.

Защита информации от несанкционированного доступа (НСД). Каналы утечки информации. Защита компонентов автоматизированных систем от НСД. Антивирусная защита. Системы анализа защищённости и обнаружения вторжений. Модель и источники каналов утечки информации.

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 разрушающих программных воздействий; понятие изолированной программной среды.

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. Парольные системы опознавания, их сущность, содержание, достоинства и недостатки. Способы повышения надежности парольных систем. Другие системы опознавания. Средства опознавания аппаратуры, программ, массивов данных.

Методы идентификации и проверки подлинности пользователей автоматизированных 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.

Биометрическая идентификация и аутентификация пользователей: основные понятия и механизмы. «Fuzzy extractors». Искусственные нейронные сети в преобразователях биометрия-код. Алгоритм быстрого обучения искусственной нейронной сети. Алгоритм ускоренного тестирования нейросетевого преобразователя биометрия-код (НПБК). Алгоритм полного тестирования НПБК. Базы биометрических образов: назначение, виды, требования к формированию. Нейросетевой биометрический контейнер (НБК): назначение, виды. Наиболее вероятные атаки на НБК, защита от них.

Программные средства разграничения доступа, их сущность, достоинства и недостатки. Модели разграничения доступа. Разграничение доступа по уровням и кольцам секретности, матрицам полномочий и мандатам. Способы и средства повышения надежности разграничения. Примеры систем разграничения доступа. Другие программные средства защиты: регистрации, сигнализации, реагирования и т.п. Программы защиты ЭВМ от электронных вирусов.

Способы организации и использования программных средств защиты.

Организационно-правовые средства защиты, их сущность, возможности, достоинства и недостатки. Критерии классификации организационно-правовых средств, классификационная структура и общая характеристика.

Система законов, регламентирующих защиту информации в РФ. Перечень основных законов, основное их содержание и порядок действия.

Руководящие методические материалы (РММ) по защите информации. Назначение и состав необходимых РММ. Перечень и содержание имеющихся РММ.

Организационные мероприятия по защите информации, их сущность и назначение.

Системная классификация организационных мероприятий. Мероприятия, проводимые на различных этапах жизненного цикла систем обработки данных.

Стеганография. Основы стеганографии. Основные понятия. Компьютерная стеганография.

4 Управление информационной безопасностью

Необходимость, сущность и основные понятия управления информационной безопасностью.

Служба информационной безопасности на объекте. Назначение и организационно-правовой статус службы. Функции и задачи службы, способы и методы их решения.

Создание, поддержка, оценка эффективности, совершенствование системы управления информационной безопасности.

Методы и модели управления рисками информационной безопасности. Формирование критериев влияния, оценивания, принятия рисков. Итерационные процедуры управления рисками информационной безопасности.

Методы и модели оценки рисков информационной безопасности. Методы идентификации рисков информационной безопасности активов. Методы формирования сценариев инцидентов, модели сценариев инцидентов. Методы идентификации и анализа последствий инцидентов различного вида. Оценка ущерба в результате нарушения безопасности. Методы оценивания рисков информационной безопасности. Методы обработки рисков информационной безопасности. Оценка вариантов обработки рисков.

Оценка эффективности выбранных защитных мер. Методы управления изменениями систем.

Управление инцидентами информационной безопасности. Обнаружение и анализ инцидентов. Методы реагирования на инциденты информационной безопасности.

Управление непрерывностью функционирования систем и объектов

Методы и модели мониторинга информационной безопасности. Структура систем мониторинга.

Методы аудита информационной безопасности. Оценка соответствия защитных мер, процессов обеспечения информационной безопасности. Методы выявления и анализа свидетельств оценки.

Организация обучения и осведомления персонала информационной безопасности.

Литература

1. Герасименко В.А. Защита информации в автоматизированных системах обработки данных: В 2 кн. М.: Радио и связь, 1999.
2. Варфоломеев А.А. Управление информационными рисками. – М.: Издательство РУДН, 2008.
3. Гатчин Ю.А., Сухостат В.В. Теория информационной безопасности и методология защиты информации. – СПб.: СПбГУ ИТМО, 2010.
4. Дорофеев А.В. Безопасный удаленный доступ к корпоративным ресурсам: Существующие концепции и решения. – М.: Мир связи, 2010 – №1-2.
5. Рыков А.С. Системный анализ, модели и методы принятия решений и поисковой оптимизации. – М.: Издательский дом МИСиС, 2009.
6. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. М.: Радио и связь, 1999.
7. Программно-аппаратные средства обеспечения информационной безопасности. Защита в операционных системах: Учеб. пособие для вузов / Проскурин В.Г., Крутов С.В., Мацкевич И.В. – М.: Радио и связь, 2000. – 168 с.

8. Государственная тайна и ее защита в Российской Федерации: Учебное пособие/Под общ.ред.М.А.Вуса и А.В.Федорова. 2-е изд., перераб. И доп.; предисловие и Н.М.Кропачева, Н.А.Сидоровой. – СПб.:Изд-во Р.Асланова «Юридический центр Пресс», 2005. – 623 с.

9. Организационно-правовое обеспечение информационной безопасности: учеб.пособие для студ. высш.учеб.заведений/А.А.Стрельцов (и др.); под ред. А.А.Стрельцова. – М.: Издательский центр «Академия», 2008. – 256 с.

10. Грушо А.А. Теоретические основы компьютерной безопасности: учеб.пособие для студентов высш.учеб.заведений/А.А.Грушо, Э.А.Применко, Е.Е.Тимонина. – М.: Издательский центр «Академия», 2009. – 272с.

11. Обеспечение информационной безопасности бизнеса/ В. В. Андрианов, С. Л. Зефиров, В. Б. Голованов, Н. А. Голдуев ; Под ред. А. П. Курило – М.: Издательство Альпина Паблишерз, 2011 – 373 с.

12. Хорев П.Б. Методы и средства защиты информации в компьютерных системах. М.: Академия, 2005.

13. Язов Ю.К. Волчихин В.И., Иванов А.И., Фунтиков В.А., Назаров И.Г. Нейросетевая защита персональных биометрических данных/ М.: Радиотехника, 2012. 157 с.

14. Волчихин В.И., Иванов А.И., Фунтиков В.А. Быстрые алгоритмы обучения нейросетевых механизмов биометрико-криптографической защиты информации. /Монография/. Пенза: Изд-во Пензенского государственного университета, 2005. 273 с.

15. ГОСТ Р ИСО/МЭК 27001 – 2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. – М.: Стандартинформ, 2006.

16. ГОСТ Р ИСО/МЭК 27002 – 2011 Информационная технология. Практические правила управления информационной безопасностью. – М.: Стандартинформ, 2011.

17. ГОСТ Р 52633.0-2006 «Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации» – М.: Стандартинформ, 2007.

Программу кандидатского экзамена разработали:

Заведующий кафедрой «Информационная безопасность систем и технологий» к.т.н., доцент С.Л. Зефиров

Профессор кафедры «Информационная безопасность систем и технологий», д.т.н., профессор Е.Д. Кашаев

Программа одобрена на заседании кафедры
«Информационная безопасность систем и технологий»
Протокол № 17 от 03 июля 2014г.

Зав. кафедрой ИБСТ С.Л. Зефиров

Секретарь кафедры А.Ю. Щербакова