МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ

МИНИСТЕРСТВО ОБРАЗОВАНИЯ, НАУКИ, КУЛЬТУРЫ И СПОРТА РА

ГОУ ВПО РОССИЙСКО-АРМЯНСКИЙ (СЛАВЯНСКИЙ) УНИВЕРСИТЕТ

Институт математики и информатики
Кафедра Математической Кибернетики

ВОПРОСЫ КАНДИДАТСКОГО МИНИМУМА ПО СПЕЦИАЛЬНОСТИ

05.13.19. «Методы и системы защиты информации, информационной безопасности»

Утверждено кафедрой Математической кибернетики
Протокол №5 от 18.02.2022 г.
зав. кафедрой
д.ф.м.н., проф., **Арамян Р. Г.**

Ереван 2022

Вопросы кандидатского минимума в аспирантуре по специальности

05.13.19. «Методы и системы защиты информации, информационной безопасности»

1. Определение и основные понятия стратегии защиты информации. Факторы, влияющие на формирование стратегий защиты. Классификационная структура множества необходимых стратегий защиты. Общая характеристика основных стратегий.
2. Определение и назначение инструментально-методологического базиса защиты информации. Требования к инструментально-методологическому базису.
3. Пути и способы реализации основных положений теории защиты информации. Перспективы и проблемы развития теории и практики защиты.
4. Определение и природа угроз информации в современных системах ее обработки. Классификация и общая характеристика основных угроз.
5. Эмпирические методы определения значений показателей уязвимости. Примеры эмпирических моделей. Способы определения параметров моделей. Особенности использования моделей.
6. Теоретико-вероятностные методы определения значений показателей уязвимости, подходы к построению моделей. Примеры моделей. Особенности и проблемы практического использования.
7. Теоретико-эмпирические методы определения значений показателей. Подходы к построению теоретико-эмпирических моделей. Понятие базового показателя уязвимости, аналитическая и статистическая модели его определения. Зависимости для определения значений обобщенных показателей уязвимости. Проблемы обеспечения моделей исходными данными и пути их решения.
8. Методы и модели прогнозирования значений показателей уязвимости. Определение, значение, структура и способы формирования инструментальных средств оценки уязвимости информации.
9. Технические средства защиты, их сущность, возможности, достоинства и недостатки. Критерии классификации и классификационная структура технических средств. Простые и сложные технические устройства защиты. Технические системы защиты. Автономные, сопряженные и встроенные технические средства.
10. Технические средства опознавания пользователей и ресурсов систем обработки данных. Параметры опознавания. Методы опознавания, способы и средства их реализации. Характеристики средств, рекомендации по использованию.
11. Программы опознавания пользователей. Парольные системы опознавания, их сущность, содержание, достоинства и недостатки. Способы повышения надежности парольных систем. Другие системы опознавания. Средства опознавания аппаратуры, программ, массивов данных.
12. 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.

13. Другие программные средства защиты: регистрации, сигнализации, реагирования и т.п. Программы защиты ЭВМ от электронных вирусов.
14. Система законов, регламентирующих защиту информации в РФ. Перечень основных законов, основное их содержание и порядок действия.
15. Организационные мероприятия по защите информации, их сущность и назначение. Системная классификация организационных мероприятий. Мероприятия, проводимые на различных этапах жизненного цикла систем обработки данных.
16. Криптографические средства защиты, их сущность, достоинства и недостатки. Основные понятия криптографического преобразования данных. Перечень и общее содержание основных методов преобразования. Характеристики криптографических способов защиты.
17. Системы (алгоритмы) криптографического преобразования данных, их назначение и принципы построения. Примеры алгоритмов. Стандартные алгоритмы и их характеристики.
18. Криптографические системы открытого ключа, их сущность и необходимость. Методы построения. Перспективные алгоритмы шифрования по методам открытого ключа.
19. Цифровая подпись, ее назначение и сущность, принципы и методы формирования. Стандарты цифровой подписи. Перспективные алгоритмы.
20. Способы и проблемы использования криптографических средств защиты в современных системах обработки данных. Криптографическое закрытие обрабатываемых и хранимых данных, данных передаваемых в сетях. Проблемы генерирования и распределения ключей.
21. Средства, основанные на применении теории графов. Графы атак для обнаружения последовательности действий, приводящих к атаке.
22. Стеганография. Основы стеганографии. Основные понятия. Компьютерная стеганография.
23. Определение и основные понятия систем защиты информации (СЗИ). Общеметодологические принципы построения СЗИ, их сущность и содержание.
24. Типизация и стандартизация архитектурного построения СЗИ. Функциональная, организационная и структурная модели СЗИ. Ядро СЗИ, его функция и состав.
25. Основы методологии проектирования СЗИ. Классификация и анализ постановок задач проектирования СЗИ. Методика выбора требований к защите информации.
26. Методика создания СЗИ на основе типовых проектных решений. Методика выбора и привязки типовой СЗИ. Методика проектирования СЗИ на базе типовых подсистем и компонентов.
27. Структура системы органов, ответственных за защиту информации. Основные функции органов государственного, регионального (ведомственного) и объектового уровней.
28. Основные положения концепции центров защиты информации (ЦЗИ). Назначение и организационно-правовой статус ЦЗИ. Основные функции ЦЗИ. Перечень и содержание услуг, оказываемых ЦЗИ своим абонентам. Примерная структура ЦЗИ. Организация работы ЦЗИ.
29. Социально-психологические аспекты защиты информации. Требования к физическому, морально-этическому и психоэмоциональному состоянию работников органов защиты информации.

30. Способы и методы подбора кадров органов защиты. Организация обучения и воспитания кадров. Способы и методы организации работы коллективов органов защиты и поддержания в них требуемого морально-психологического климата.

Литература

1. Виноградов И.М. Основы теории чисел. Москва-Ижевск. НИЦ «Регулярная и хаотическая динамика», 2003
2. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. М.: Радио и связь, 1999.
3. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности СВТ от НСД к информации. Руководящий документ Гостехкомиссии России. М.: ГТК РФ, 1992.
4. Герасименко В.А. Защита информации в автоматизированных системах обработки данных: В 2 кн. М.: Радио и связь, 1999.
5. Ященко В.В. Введение в криптографию. М., 2001
6. Гене О.В. Основные положения стеганографии. М., 2000
7. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. М., 2002
8. Мелик-Шахназаров Б.Б. Информационные основы теории управления. Ереван, РАУ, 2003
9. Таирян В.И. Введение в алгебраическую теорию кодирования. Ереван, РАУ, 2003
10. Таирян В.И. Основы информационной безопасности в компьютерных сетях. Ереван, РАУ, 2006
11. Таирян В.И., Таирян С.В., Берберян Л.С. Обеспечение информационно-психологической безопасности методами социальной инженерии и стеганографии. Ереван, РАУ, 2010
12. Авторский коллектив, рук. Таирян В.И. Экспертные методы в задачах информационно-психологической безопасности систем. Ереван, «ВАН АРЬЯН», 2011
13. Авторский коллектив, рук. Таирян В.И. Математические и практические основы обеспечения информационной безопасности. Ереван, 2010
14. Таирян В.И., Таирян С.В., Абрамян А.А., Таирян М.В. Управление информационно-психологической безопасностью банковских систем. Ереван, РАУ, 2011