Автономная некоммерческая организация
"Институт инженерной физики"

УТВЕРЖДАЮ
Президент
Заслуженный деятель науки РФ
доктор технических наук, профессор
А.Н. Царьков
«__» апреля 2022 г.

ПРОГРАММА

кандидатского экзамена по научной специальности
2. 3.6. «Методы и системы защиты информации, информационная безопасность»
по техническим наукам

Часть 1

Программа кандидатского экзамена рассмотрена и рекомендована к утверждению на заседании научно-технического Совета АНО «Институт инженерной физики», протокол № 4 от 08.04.2022 г.

Серпухов, 2022

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.

Программа разработана экспертным советом Высшей аттестационной комиссии Министерства образования Российской Федерации по управлению, вычислительной технике и информатике при участии Московского государственного горного университета, Московского энергетического института (технического университета) и Института системного анализа РАН.

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, надёжность 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 дешифрования 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 защищённых компьютерных систем нового поколения на основе СИИТ.

3. Список вопросов для кандидатского экзамена

3.1. Методы и системы защиты информации

1. Определение, особенности и общее содержание теории защиты информации. Научно-методический базис теории защиты.
2. Система моделей защиты информации.
3. Факторы, влияющие на формирование стратегий защиты. Общая характеристика основных стратегий.
4. Определение и назначение инструментально методологического базиса защиты информации. Требования к инструментально-методологическому базису.
5. Структура и общее содержание унифицированной концепции защиты информации.
6. Система концептуальных решений по защите информации.
7. Технические средства защиты, их сущность, возможности, достоинства и недостатки.
8. Критерии классификации и классификационная структура технических средств. Автономные, сопряженные и встроенные технические средства.
9. Программы аутентификации пользователей. Парольные системы аутентификации, их сущность, содержание, достоинства и недостатки.
10. Программы защиты ЭВМ от электронных вирусов.
11. Криптографические средства защиты, их сущность, достоинства и недостатки. Основные понятия криптографического преобразования данных.

12. Криптографические системы с открытым ключом, их сущность и необходимость. Методы построения.

13. Перспективные алгоритмы шифрования с открытым ключом.

14. Электронная подпись, её назначение и сущность, принципы и методы формирования. Стандарты электронной подписи.

15. Шифры перестановки. Поточные шифры замены. Блочные шифры простой замены и особенности их анализа.

16. Криптоалгоритм ГОСТ-28147-89.

17. Криптоалгоритм RIJNDAEL.

18. Общеметодологические принципы построения систем защиты информации (СЗИ), их сущность и содержание.

19. Основы архитектурного построения СЗИ. Функциональная, организационная и структурная модели СЗИ.

20. Ядро СЗИ, его функции и состав. Типизация и стандартизация архитектурного построения СЗИ.

21. Основы методологии проектирования СЗИ. Классификация и анализ постановок задач проектирования СЗИ.

22. Методика выбора требований к защите информации. Методика создания СЗИ на основе типовых проектных решений.

23. Методика оптимального выбора задач, необходимых для осуществления функций защиты.

24. Методика выбора средств защиты, необходимых и достаточных для эффективного решения выбранных средств защиты. Методика объединения выбранных средств в СЗИ.

25. Теоретико-вероятностные методы определения значений показателей уязвимости, подходы к построению моделей.

26. Теоретико-эмпирические методы определения значений показателей. Подходы к построению теоретико-эмпирических моделей.

27. Понятие базового показателя уязвимости, аналитическая и статистическая модели его определения. Зависимости для определения значений обобщенных показателей уязвимости.

28. Основные понятия и определения теории информационно-телекоммуникационных систем (ИТКС): сети передачи данных, мультиплексирование, сети с коммутацией каналов и пакетов, протоколы и архитектура сетей.

29. Использование радиосредств в ИТКС: организация стационарного радиодоступа к телефонным сетям и к подвижным абонентам, стандарты сотовых систем подвижной радиосвязи. 30. Основные принципы построения систем сотовой связи. Информационная безопасность систем мобильной связи.

31. Методика построения защищенных компьютерных систем.

32. Анализ рисков и выбор направлений защиты компьютерных систем. Разработка системы организационных и физических мер защиты компьютерных систем.

33. Разработка системы программно-технических мер защиты компьютерных систем.

34. Нейтрализация угроз и уязвимых мест компьютерных систем. Защита компьютерных систем от персонала.

35. Особенности защиты информации в базах данных. Защищённые файловые системы.

36. Защита в СУБД. Защита баз данных в сетях ЭВМ. Протоколы и процедуры передачи файлов.

37. Динамическая защита баз данных.

38. Контекстно-ориентированная защита.

39. Доступ к электронным документам и порядок эффективного закрытия его для обеспечения безопасности информации на рабочих местах в организации.

40. Порядок заключения договоров об обмене электронными документами.

41. Электронная цифровая подпись. Получение сертификата электронной цифровой подписи.

42. Условия применения электронной цифровой подписи при подписании документов. Реализация схемы цифровой метки.

43. Принципы и средства защитных преобразований сигналов при передаче аналоговых и дискретных сигналов. Спектральные, временные и комбинированные преобразования.

44. Проблема защиты служебных сигналов при передаче.

45. Симметричное и асимметричное шифрование в задачах защиты информации электронного документооборота.

46. Модели шифров. Простейшие криптографические протоколы.

47. Характеристики имитостойкости шифров и их оценки. Параметры имитостойких и неимитостойких шифров.

48. Шифры, не размножающие искажений типа замены знаков.

49. Шифры, не размножающие искажений типа пропуск-вставка знаков для систем документооборота.

50. Системы шифрования с открытым ключом. Алгоритмы цифровых подписей.

51. Цифровые подписи на основе шифросистем с открытым ключом.

52. Цифровая подпись Фиата-Шамира. Цифровая подпись Эль-Гамаля.

53. Алгоритмы распределения ключей. Алгоритмы передачи ключей (с использованием и без использования цифровой подписи).

54. Шифросистема Эль-Гамаля.

55. Шифросистема на основе задачи об «укладке рюкзака».

56. Анализ шифросистемы RSA.

57. Практические аспекты использования шифросистем с открытым ключом в системах электронного документооборота.

3.2. Информационная безопасность

1. Централизация управления информационными ресурсами.

2. Двух- и трёхуровневые клиент-серверные системы.

3. Многоуровневые клиент-серверные системы.

4. Принципы разделения и изоляции этапов информационного взаимодействия с позиции безопасности

5. Структура информационной системы с Web-доступом.

6. Распределенные серверы приложений и бизнез-логика.

7. Технология вызова удаленных процедур.

8. Современные технологии разработки клиент-серверных приложений. Технология NET Remoting.

9. Современные технологии разработки клиент-серверных приложений. Технологии ASP, ASP .NET.WEB-сервисы.

10. Современные технологии разработки клиент-серверных приложений. XML – технологии. Протокол SOAP.

11. Проблемы безопасного использования клиентских и серверных сценариев, ActiveX-объектов и апплетов.

12. Принципы и приемы разработки компонентов безопасных приложений.

13. Высокоуровневые программные интерфейсы доступа к серверам баз данных – (ODBC, ADO, ADO.NET).

14. Методы защиты серверов баз данных.

15. Методы обеспечения безопасности информационного взаимодействия между программными компонентами информационных систем.

16. Протоколы взаимной аутентификации шифрования данных.

17. Основные проблемы обеспечения безопасности доступа при использовании беспроводных каналов передачи данных.

18. Протоколы аутентификации и шифрования данных в беспроводных сетях.

4. Основная литература

1. Бабенко Л.К., Ищукова Е.А. Криптографическая защита информации: симметричное шифрование. Учебное пособие для ВУЗов. – М.: Юрайт, 2018. – 220 с.

2. Грибунин В.Г. Комплексная система защиты информации на предприятии. М.: Академия, 2009. – 416 с.

3. Гришина Н.В. Организация комплексной системы защиты информации. – М.: Гелиос АРВ, 2007. – 256 с.

4. Зайцев А.П. Технические средства и методы защиты информации.-М.: Горячая линия – Телеком, 2009. – 616 с.

5. Куприянов А.И. Основы защиты информации. – М.: Академия, 2006. – 256 с.

6. Зайцев А.П. Технические средства и методы защиты информации: учебник для вузов / А.П. Зайцев, Р.В. Мещеряков, А.А. Шелупанов; под ред. А.П. Зайцева, А.А. Шелупанова. – 7-е изд., испр. – М.: Горячая линия-Телеком, 2016. – 442 с.

7. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. – М.: Горячая линия – Телеком, 2004, – 280 с.

8. Партыка Т.Л. Информационная безопасность. – М.: Инфра-М, 2007. – 368 с.

9. Щеглов Ю.А. Защита компьютерной информации от несанкционированного доступа. – М.: Наука и техника, 2008. – 384 с.

10. Щеглов А.Ю. Защита информации: основы теории: учебник для бакалавриата и магистратуры / А.Ю. Щеглов, К.А. Щеглов. – М.: Юрайт, 2018. – 309 с.

11. Фомичёв В.М. Криптографические методы защиты информации. В 2 ч. Часть 1. Математические аспекты: учебник для академического бакалавриата / В.М. ФОМИЧЕВ, Д.А. Мельников. – М.: Юрайт, 2017. – 209 с.

12. Фомичёв В.М. Криптографические методы защиты информации. В 2 ч. Часть 2. Системные и прикладные аспекты: учебник для академического бакалавриата / В.М. Фомичёв, Д.А. Мельников. – М.: Юрайт, 2017. – 245 с.

13. Фомичёв В.М. Дискретная математика и криптология. 2-е изд. – М.: ДИАЛОГ-МИФИ, 2006. – 400 с.

14. Харин Ю.С. Математические и компьютерные основы криптологии. – М.: Новое знание, 2003. – 382 с.

15. Басалова Г.В. Основы криптографии [Электронный ресурс], – http://biblioclub.ru/index.php?page=book&id=233689.

16. Галатенко, В.А. Основы информационной безопасности: Курс лекций : учебное пособие / В.А. Галатенко; под ред. В.Б. Бетелина. – Изд. 3-е. – М.: Интернет-Университет Информационных Технологий, 2006. – 208 с. [Электронный ресурс]. – URL: http://biblioclub.ru/index.php?page=book&id=233063.

17. Креопалов В.В. Технические средства и методы защиты информации [ресурс], – http://biblioclub.ru/index.php?page=book&id=90753.

18. Лидовский В.В. Основы теории информации и криптографии [Электронный ресурс], – https://biblioclub.ru/index.php?page=search_red.

19. Технологии защиты информации в компьютерных сетях / Н.А. Руденков, А.В. Пролетарский, Е.В. Смирнова, А.М. Суровов. – 2-е изд., испр. – М.: Национальный Открытый Университет «ИНТУИТ», 2016. – 369 с. [Электронный ресурс]. – URL: http://biblioclub.ru/index.php?page=book&id=428820.

Дополнительная литература

1. ГОСТ Р 50992-96. Защита информации. Основные термины и определения.

2. ГОСТ Р 51583-2000.Порядок создания автоматизированных систем в защищёном исполнении.

3. Рекомендации по стандартизации Р 50.1.053-2005. Информационные технологии, Основные термины и определения в области технической защиты информации.

4. Белов Е.Б. Основы информационной безопасности. – «Телеком», 2006. – 544 с.

5. Внуков А.А. Защита информации: учебное пособие для бакалавриата и магистратуры. 2-е изд., испр. и доп. – М.: Юрайт, 2018. – 261 с.

6. Романов О.А., Бабин С.А., Жданов С.Г. Организационное обеспечение информационной безопасности. – М.: ИЦ Академия, 2008. – 192 с.

7.Программно-аппаратные средства обеспечения информационной безопасности: учебное пособие для вузов/ под. ред. А.В. Душкина. М.: Горячая линия – Телеком. 2018. – 248 с.

8. Сёмкин К.Н. и др. Основы организационного обеспечения информационной безопасности объектов информатизации. – М.: Гелиос АРВ, 2005. – 192 с.

9. Хорев П.Б. Методы и средства защиты информации в компьютерных системах. М.: Академия, 2006. – 256 с.

10. Галатенко В.А. Стандарты информационной безопасности [Электронный ресурс], – http://biblioclub.ru/index.php?page=book&id=233065

Автор программы:
Главный научный сотрудник отдела
специальных средств и систем
защиты информации МОУ «ИИФ»
доктор технических наук _____ В. Г. Грибунин

Согласовано:
Вице-президент Института по инновационным проектам,
руководитель аспирантуры
д.т.н., профессор _____ И. А. Бугаков
«14» апреля 2022 г.