МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«РОСТОВСКИЙ ГОСУДАРСТВЕННЫЙ ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ
(РИНХ)»

ПРИНЯТО
Решением Научно-методического совета
ФГБОУ ВО «РГЭУ (РИНХ)»
от «27» 03 2024 г., протокол № 2

«УТВЕРЖДАЮ»
Проректор по научной работе
и инновациям
_____ Н.Г. Вовченко
«___» _____ 2024 г.

ПРОГРАММА КАНДИДАТСКОГО ЭКЗАМЕНА
по специальной дисциплине
«МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Научная специальность
2.3.6. Методы и системы защиты информации, Информационная безопасность

Наименование отрасли науки,
по которой присуждаются ученые степени:
технические науки

Ростов–на–Дону – 2024

Программа разработана на кафедре информационной безопасности.

И.о. зав. кафедрой ИБ
к.э.н., доцент Ю.В. Радченко

Составители:
профессор кафедры ИБ д.э.н., профессор Е.Н. Тищенко
доцент кафедры ИБ к.т.н., доцент О.В. Серпенинов

Рецензент:
профессор кафедры ИБ д.т.н., профессор С.В. Соколов

ВВЕДЕНИЕ

Программа предназначена для аспирантов очной формы, обучающихся по научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность, а также для лиц, прикрепленных для сдачи кандидатских экзаменов без освоения программы подготовки научных и научно-педагогических кадров в аспирантуре. Программа ориентирована на выявление профессионального уровня обучающихся, степени их готовности к научной работе, широты диапазона аналитического и ассоциативного мышления. Программа кандидатского экзамена составлена на основании Паспорта научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Кандидатский экзамен по специальной дисциплине «Методы и системы защиты информации, информационная безопасность» проводится в устной форме по билетам. В каждом билете три вопроса:

– **1-й и 2-й вопросы** из перечня вопросов к кандидатскому экзамену по специальной дисциплине «Методы и системы защиты информации, информационная безопасность»;

– **3-й вопрос** по теме научного исследования аспиранта и сформулирован в следующей редакции: «Перечислите и опишите актуальные проблемы Вашей области исследований и роль Вашего исследования в решении этих проблем».

СОДЕРЖАНИЕ ПРОГРАММЫ

1. Методы и системы защиты информации

1.1 Законодательные и правовые основы защиты компьютерной информации и 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.

1.2 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.

1.3 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

2.1 Изучение традиционных симметричных криптосистем.

Основные понятия и определения; шифры перестановки;

шифр перестановки «сцитала»; 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.

2.2 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.

2.3 Применение ассиметричных криптосистем для защиты компьютерной информации в информационных системах.

Концепция криптосистемы с открытым ключом;

однонаправленные функции; криптосистема шифрования 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.

2.4 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.

2.5 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 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.

2.6 Методы защита 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.

2.7 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.

РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

Основная литература

1. Хорев А.А. Техническая защита информации: Учебное пособие для студентов. В 3 т. Т.1. Технические каналы утечки информации. - М.: Аналитика, 2008.
2. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах: Учебное пособие. - М.: Форум; Инфра-М, 2012.
3. Аттестационные испытания автоматизированных систем от несанкционированного доступа по требованиям безопасности информации: Учебное пособие / В.С. Горбатов, СВ. Дворянкин, А.П. Дураковский, Р.С. Енгалычев [и др.], под общ. ред. Ю.Н. Лаврухина. - М: НИЯУ МИФИ, 2014.-560 с.
4. Контроль защищенности информации от утечки по техническим каналам за счет побочных электромагнитных излучений и наводок. Аттестационные испытания по требованиям безопасности информации: Учебное пособие / А.А. Голяков, В.С. Горбатов, А.П. Дураковский, А.Е. Панин, М.С. Чистяков; под общ. ред. Ю.Н., Лаврухина. - М: НИЯУ МИФИ, 2014. - 208 с: ил.
5. Контроль защищенности речевой информации в помещениях. Аттестационные испытания выделенных помещений по требованиям безопасности информации: Учебное пособие / В.С. Горбатов, А.П. Дураковский, И.В. Куницын, А.Е. Панин, под общ. ред. Ю.Н. Лаврухина. - М: НИЯУ МИФИ, 2014. - 248 с: ил.
6. Технические средства и методы защиты информации: Учебное пособие для вузов / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков; под ред. А.П. Зайцева и А.А. Шелупанова. - 7-е изд. испр. - М.: Горячая линия - Телеком, 2012.
7. Правовой режим лицензирования и сертификации в сфере информационной безопасности: Учебное пособие / Ю.Ю. Коваленко. - М.: Горячая линия - Телеком, 2012.
8. Концептуальные основы создания и применения системы защиты объектов / В.А. Воронов, В.А. Тихонов. - М.: Горячая линия - Телеком, 2013.
9. Грибунин В.Г. Комплексная система защиты информации на предприятии: Учебное пособие. - М.: Академия, 2009.
10. Гришина Н.В. Комплексная система защиты информации на предприятии: Учебное пособие. - М: Форум, 2013.
11. Методический документ. Меры защиты информации в государственных информационных системах. Утвержден ФСТЭК России 11 февраля 2014 г.
12. Безопасность глобальных сетевых технологий. - 2-е изд. / В.М. Зима, А.А. Молдовян, Н.А. Молдовян. - СПб.: БХВ-Петербург, 2014. - 368 с;
13. Соколов С.В., Серпенинов О.В., Тищенко Е.Н. Криптографическая защита информации. Учебное пособие. – Ростов н/Д: РГЭУ (РИНХ), 2011. – 251 с.
14. Серпенинов О.В. Организация аттестации объектов ТСПИ. Учебно-методическое пособие. - Ростов н/Д, РВИ РВ, 2010.
15. Шейдаков Н.Е., Серпенинов О.В., Тищенко Е.Н. Физические основы защиты информации: Учебное пособие. – М.: РИОР: ИНФРА-М, 2016. – 204 с.

Дополнительная литература

1. Федеральный закон от 28.12.2010 № 390-ФЗ «О безопасности».
2. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
3. Федеральный закон от 27.12.2002 № 184-ФЗ «О техническом регулировании».
4. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
5. Федеральный закон от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности».
6. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
7. Федеральный закон от 06.04.2011 № 63 «Об электронной подписи».
8. Указ Президента Российской Федерации от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации».
9. Указ Президента Российской Федерации от 17.03.2008 №351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».
10. Указ Президента Российской Федерации от 05.12.2016 № 646 «Доктрина информационной безопасности Российской Федерации».
11. Указ Президента Российской Федерации от 16.08.2004 № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».
12. Указ Президента Российской Федерации от 9.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы».
13. Постановление Правительства Российской Федерации от 21.11.2011 № 957 «Об организации лицензирования отдельных видов деятельности».
14. Постановление Правительства Российской Федерации от 03.02.2012 № 79 «О лицензировании деятельности по технической защите конфиденциальной информации».
15. Постановление Правительства Российской Федерации от 15.04.1995 № 333 «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны».
16. Постановление Правительства Российской Федерации от 26.06.1995 № 608 «О сертификации средств защиты информации».
17. Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
18. Постановление Правительства Российской Федерации от 08.02.2018 № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений».

19. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.

20. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

21. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.

22. ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Ростехрегулирование, 2008.

23. ГОСТ Р 51241-2008 Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний. Ростехрегулирование, 2008.

24. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Госстандарт, 2012.

25. ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности. Росстандарт, 2013.

26. ГОСТ Р ИСО/МЭК 15408-3-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности. Росстандарт, 2013.

27. ГОСТ Р 56545-2015 Защита информации. Уязвимости информационных систем. Правила описания уязвимости. Росстандарт, 2015.

28. ГОСТ Р 56546-2015 Защита информации. Уязвимости информационных систем. Классификация уязвимости информационных систем. Росстандарт, 2015.

29. Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

30. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

31. Приказ ФСТЭК России от 21.12.2017 № 235 «Об утверждении требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования».

32. Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

33. Приказ ФСТЭК России от 03.04 2018 № 55 «Об утверждении Положения о системе сертификации средств защиты информации».

34. Приказ ФСТЭК России от 29.04.2021 № 77 «Об утверждении Порядка

организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну».

35. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 15.02.2008.

36. Методический документ. Методика оценки угроз безопасности информации. Утвержден ФСТЭК России 05.02.2021.

БАЗЫ ДАННЫХ, ИНФОРМАЦИОННО-СПРАВОЧНЫЕ И ПОИСКОВЫЕ СИСТЕМЫ

1. Информационно-правовая система «Законодательство России» // Официальный интернет-портал правовой информации – URL: http:// www.pravo.gov.ru;

2.Официальный сайт ФСТЭК России – URL: http:// www.fstec.ru; банк данных угроз безопасности информации – URL: http://bdu.fstec.ru;

3.Каталог стандартов // Официальный сайт Росстандарта – URL: http://www.gost.ru/wps/portal/pages.CatalogOfStandarts;

4.Правовые справочно-поисковые системы («Гарант», «Консультант Плюс»).

ПЕРЕЧЕНЬ ВОПРОСОВ К КАНДИДАТСКОМУ ЭКЗАМЕНУ ПО СПЕЦИАЛЬНОЙ ДИСЦИПЛИНЕ «МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

1. Стратегические цели и основные направления обеспечения информационной безопасности РФ.
2. Законодательно – правовые и организационные основы обеспечения защиты информации.
3. Организация защиты информации на предприятии.
4. Выбор показателей эффективности и критериев оптимальности комплексной системы защиты информации.
5. Моделирование комплексной системы защиты информации.
6. Политика безопасности предприятия.
7. Синтез системы защиты информации. Разработка технического задания.
8. Структура системы государственного лицензирования.
9. Лицензионные требования и условия в области защиты информации.
10. Структура системы сертификации в области защиты информации.
11. Порядок сертификации средств защиты информации.
12. Порядок проведения аттестации объектов информатизации.
13. Аттестация объектов информатизации. Подготовка исходных данных.
14. Аттестация объектов информатизации. Оформление результатов аттестации.
15. Законодательство РФ о государственной тайне. Полномочия органов государственной власти и должностных лиц.
16. Порядок засекречивания и рассекречивания сведений и их носителей.

17. Порядок допуска к государственной тайне.
18. Правила отнесения сведений, составляющих государственную тайну, к различным степеням секретности.
19. Организация допуска должностных лиц и граждан к государственной тайне.
20. Организация и порядок проведения специальных экспертиз предприятий.
21. Коммерческая тайна как вид защищаемой конфиденциальной информации.
22. Охрана коммерческой тайны в рамках трудовых отношений.
23. Организация контроля за обеспечением режима при работе со сведениями, содержащими коммерческую тайну.
24. Состав и структура системы безопасности предприятия.
25. Правовые основы деятельности службы безопасности.
26. Силы и средства, используемые при организации внутриобъектового режима.
27. Основные элементы системы организации пропускного режима.
28. Оценка и управление рисками. Экономическая оценка систем и средств защиты.
29. Технические методы и средства защиты информации от утечки по техническим каналам.
30. Методы защиты информации от несанкционированного доступа.
31. Обеспечение информационной безопасности при вводе объектов в эксплуатацию.
32. Выбор и оптимизация требуемых средств защиты информации на объектах.
33. Классификация методов зашиты информации от программно-математических воздействий.
34. Деятельность администратора безопасности по предотвращению программно-математических воздействий.
35. Формирование требований к защите информации в информационной системе.
36. Определение класса защищенности информационной системы.
37. Требования к мерам защиты информации в информационной системе.
38. Модель угроз безопасности информации в информационной системе.
39. Модель нарушителя в информационной системе.
40. Аттестация информационной системы и ввод ее в действие.
41. Аудит состояния информационной безопасности на объектах информатизации.
42. Методы экспертного анализа состояния информационной безопасности на объектах информатизации.
43. Виды контроля состояния информационной безопасности объектов.
44. Объектовый мониторинг состояния информационной безопасности.
45. Формы представления результатов контроля информационной безопасности.
46. Методы оценки эффективности мероприятий информационной безопасности.

47. Расчетно-аналитические методы оценки эффективности систем информационной безопасности.

48. Средства управления безопасностью локальных сетей.

49. Аппаратная защита электронного обмена информацией

50. Нормативно-правовое обеспечение защиты персональных данных.

51. Требования к защите персональных данных при их обработке в ИСПДн.

52. Принципы и условия обработки ПДн. Обязанности оператора ПДн.

53. Порядок организации защиты ПДн. Состав и содержание мер по обеспечению безопасности ПДн.

54. Основные положения базовой модели угроз безопасности ПДн при их обработке в ИСПДн.

55. Законодательно-правовые акты, регулирующие деятельность по организации защиты объектов КИИ.

56. Порядок формирования перечня объектов КИИ.

57. Основные этапы категорирования объектов КИИ.

58. Техническая реализация аппаратных средств защиты информации

59. Архитектура семейства технических устройств аппаратной защиты информации

60. Управление рисками. Модель безопасности с полным перекрытием

61. Современные стандарты в области информационной безопасности, использующие концепцию управление рисками.

62. Основные направления использования современной криптографии.

63. Основные требования к криптосистемам.

64. Классификация методов криптографического преобразования информации.

65. Структура алгоритма DES. Анализ особенностей блоков начальной и заключительной перестановок.

66. Принцип построения схемы шифрования с открытым ключом.

67. Принцип построения схемы электронной цифровой подписи.

68. Практическая стойкость криптосистемы и параметры, ее характеризующие.

69. Структура алгоритма шифрования RSA. Условия его работоспособности и их теоретическое обоснование.

70. Организация криптосистем на основе канального и сквозного шифрования. Основные преимущества и недостатки обоих типов шифрования.

71. Преступления в сфере компьютерной информации. Признаки и элементы состава преступления.

КРИТЕРИИ ОЦЕНИВАНИЯ НА КАНДИДАТСКОМ ЭКЗАМЕНЕ:

- оценка «**отлично**» выставляется, если изложенный материал фактически верен, характеризуется наличием глубоких исчерпывающих знаний по программе кандидатского экзамена по специальной дисциплине; правильные, уверенные действия по применению полученных знаний на практике; аргументировано доказана научная новизна и практическая значимость проведенного исследования; грамотное и логически стройное изложение материала при ответе; продемонстрировано усвоение основной и знакомство с дополнительной литературой;
- оценка «**хорошо**» - наличие твердых и достаточно полных знаний по программе кандидатского экзамена по специальной дисциплине; правильные действия по применению знаний на практике; четкое изложение материала, допускаются отдельные логические и стилистические погрешности; обоснованы пункты научной новизны и практическая значимость проведенного исследования; продемонстрировано усвоение основной литературы, рекомендованной в программе кандидатского экзамена;
- оценка «**удовлетворительно**» - наличие твердых знаний по программе кандидатского экзамена по специальной дисциплине; изложение ответов с отдельными ошибками, уверенно исправленными после дополнительных вопросов; правильные в целом действия по применению знаний на практике;
- оценка «**неудовлетворительно**» - ответы не связаны с вопросами, наличие грубых ошибок в ответе, непонимание сущности излагаемого вопроса, неумение применять знания на практике, неуверенность и неточность ответов на дополнительные и наводящие вопросы.