МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

**«УФИМСКИЙ ГОСУДАРСТВЕННЫЙ АВИАЦИОННЫЙ
ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

Кафедра *вычислительной техники и защиты информации*

УТВЕРЖДАЮ

Первый проректор по науке

_____Р.Д. Еникеев

«23» июня 2022 г.

ПРОГРАММА

КАНДИДАТСКОГО ЭКЗАМЕНА

ПО НАУЧНОЙ СПЕЦИАЛЬНОСТИ
2.3.6. *Методы и системы защиты информации, информационная безопасность*

Уровень подготовки
высшее образование - подготовка научных и научно-педагогических кадров в аспирантуре

Квалификация (ученая степень): кандидат наук

Форма обучения
очная

Уфа 2022

Программа кандидатского экзамена по научной специальности

2.3.6. *Методы и системы защиты информации, информационная безопасность*

Программа кандидатского экзамена *обсуждена на заседании кафедры ВТиЗИ* 08.04.2022 *г., протокол №* 11 *и рекомендована к реализации в образовательном процессе для подготовки аспирантов по ПА2.3.6 «Методы и системы защиты информации, информационная безопасность».*

Заведующий кафедрой: _____ В.М. Картак

Составитель: _____ В.В. Сагитова, к.т.н., старший преподаватель кафедры ВТиЗИ

Согласовано: _____ Р.К. Фаттахов, к.т.н., доцент, начальник ОАиД

Содержание

1. Общие положения

Кандидатский экзамен по специальности по программе аспирантуры - подготовка научных и научно-педагогических кадров в аспирантуре является обязательным. Кандидатский экзамен проводится экзаменационными комиссиями. Целью кандидатского экзамена по специальности является – определение уровня подготовленности соискателя к самостоятельной научно-исследовательской работе.

Место кандидатского экзамена по специальности в программе аспирантуры подготовки научных и научно-педагогических кадров в аспирантуре.

Кандидатский экзамен по специальности проводится на 3 курсе в 5 семестре.

2 Содержание кандидатского экзамена по специальности

Основу настоящей программы составили ключевые положения следующих дисциплин:

- Методы и системы защиты информации, информационная безопасность

Перечень вопросов

1. Законодательные и правовые основы защиты компьютерной информации информационных технологий.
2. Безопасность информационных ресурсов и документирование информации.
3. персональные данные о гражданах.
4. Вычислительные сети и защита информации; нормативно-правовая база функционирования систем защиты информации.
5. Российское законодательство по защите информационных технологий.
6. Правовая защита программного обеспечения авторским правом.
7. Проблемы защиты информации в информационных системах.
8. Меры по обеспечению сохранности информации и угрозы ее безопасности в информационных системах.
9. защита локальных сетей и операционных систем.
10. Internet в структуре информационно-аналитического обеспечения информационных систем; рекомендации по защите информации в Internet.
11. Содержание системы средств защиты компьютерной информации в информационных системах.
12. Защищенная информационная система и система защиты информации.
13. законодательная, нормативно-методическая и научная база системы защиты информации.
14. Требования к содержанию нормативно-методических документов по защите информации.
15. Организационно-правовой статус службы информационной безопасности; организационно-технические и режимные меры.
16. Политика безопасности.
17. Программно-технические методы и средства защиты информации.
18. Программно-аппаратные методы и средства ограничения доступа к компонентам компьютера.
19. Типы несанкционированного доступа и условия работы средств защиты.
20. Симметричные криптосистемы: основные понятия и определения.
21. Применение симметричных криптосистем для защиты компьютерной информации в информационных системах.
22. Изучение американского стандарта шифрования данных DES.
23. Отечественный стандарт шифрования данных; режим простой замены.
24. Режим гаммирования; режим гаммирования с обратной связью.
25. Режим выработки имитовставки; блочные и поточные шифры.
26. Применение асимметричных криптосистем для защиты компьютерной информации в информационных системах.
27. Концепция криптосистемы с открытым ключом.

28. Криптосистема шифрования данных RSA (процедуры шифрования и расшифрования в этой системе).
29. Схема шифрования Полига—Хеллмана.
30. Схема шифрования Эль-Гамаля.
31. Методы идентификации и проверки подлинности пользователей компьютерных систем. проблема аутентификации данных и электронная подпись.
32. Однонаправленные хэш-функции на основе симметричных блочных алгоритмов.
33. Отечественный стандарт хэш-функции.
34. Алгоритм цифровой подписи RSA.
35. Алгоритм цифровой подписи Эль-Гамаля (EGSA).
36. Алгоритм цифровой подписи DSA.
37. Отечественный стандарт цифровой подписи.
38. Защита компьютерных систем от удаленных атак через сеть Internet.
39. Изучение существующих аппаратно-программных средств криптографической защиты компьютерной информации серии КРИПТОН.
40. Программно-аппаратная система защиты от несанкционированного доступа (НСД) КРИПТОН-ВЕТО.
41. Защита от НСД со стороны сети; абонентское шифрование и ЭП.
42. Методы защиты программ от изучения и разрушающих программных воздействий (программных закладок и вирусов).
43. Классификация способов защиты; защита от отладок и дизассемблирования.
44. Способы встраивания защитных механизмов в программное обеспечение.
45. Комплексная защита процесса обработки информации в компьютерных системах на основе стохастической интеллектуальной информационной технологии.
46. Метод защиты от НСД и разрушающих программных воздействий процесса хранения, обработки информации; защита арифметических вычислений в компьютерных системах.
47. Список практических вопросов и задач на экзамене по дисциплине.
48. Алгоритмы шифрования последовательности блоков методами DES, ГОСТ 28147-89 во всех режимах.
49. Алгоритмы многораундового шифрования блока методами DES, ГОСТ 28147-89 во всех режимах.
50. Операции, применяемые для шифрования блока в раунде методами DES, ГОСТ 28147-89.
51. Алгоритмы шифрования блока в раунде методами DES, ГОСТ 28147-89.
52. Алгоритмы выработки ключа для шифрования блока в раунде методами DES, ГОСТ 28147-89.
53. Операции в конечном поле GF(28) (умножение, сложение и т.д.).
54. Алгоритм многораундового шифрования методом Rijndael.
55. Алгоритм раундового преобразования при шифровании Rijndael.
56. Операции раундового преобразования и их реализация.
57. Алгоритм выработки раундовых ключей при шифровании Rijndael.
58. Выработка открытого ключа для шифрования алгоритмом RSA. Алгоритм шифрования и подписывания методом RSA.
59. Определение секретного ключа по открытому ключу в алгоритме RSA. Алгоритмы определения взаимной простоты чисел (e и n) и поиска обратного элемента e-1 mod n.
60. Алгоритм поиска примитивных элементов в поле GF(P). Алгоритм Диффи-Хэллмана выработки общего секретного ключ.

Критерии выставления оценок на государственном экзамене

Критерии оценки:

«Отлично» – продемонстрированы достаточно твердые знания материала по основным вопросам, проявлено внимание сущности и взаимосвязи рассматриваемых процессов и явлений,

даны правильные полные ответы на большинство вопросов. Нет грубых ошибок, при ответах на некоторые вопросы допущены неточности.

«Хорошо» – продемонстрированы достаточно твердые знания материала по основным вопросам, однако, не уделено достаточного внимания сущности и взаимосвязи рассматриваемых процессов и явлений, даны правильные полные ответы на большинство вопросов. Нет грубых ошибок, при ответах на половину вопросов допущены неточности.

«Удовлетворительно» – продемонстрированы недостаточно твердые знания материала по основным вопросам, не уделено достаточного внимания сущности и взаимосвязи рассматриваемых процессов и явлений, частично даны правильные полные ответы на вопросы. Есть грубые ошибки, при ответах на некоторые вопросы допущены неточности.

«Неудовлетворительно» – не дано ответа или даны неправильные ответы на большинство вопросов, продемонстрировано непонимание сущности предложенных вопросов, допущены грубые ошибки при ответе на вопросы, компетенции не сформированы полностью или частично.

Порядок проведения экзамена

Экзамен проводится путем сочетания письменной и устной форм. Каждый билет включает 3 теоретических вопроса, 2 вопроса, непосредственно связанных с темой и разработками диссертационной работы в области математического и программного обеспечения вычислительных машин, комплексов и компьютерных сетей.

На экзамене разрешается использовать материалы справочного характера.

Все члены экзаменационной комиссии слушают ответ экзаменуемого и оценивают его знания. Решение об итоговой оценке знаний аспиранта принимается комиссией на закрытом заседании открытым голосованием большинства голосов членов комиссии, участвующих в голосовании. При равном числе голосов решающим является голос председателя. Результаты сдачи государственного экзамена объявляются в тот же день после оформления в установленном порядке протоколов заседаний экзаменационных комиссий.

3. Перечень рекомендуемой литературы

1. Краковский, Ю. М. Методы защиты информации : учебное пособие для вузов / Ю. М. Краковский. — 3-е изд., перераб. — Санкт-Петербург : Лань, 2021. — 236 с. — ISBN 978-5-8114-5632-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/156401

2. Нестеров, С. А. Основы информационной безопасности : учебник для вузов / С. А. Нестеров. — Санкт-Петербург : Лань, 2021. — 324 с. — ISBN 978-5-8114-6738-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com2/book/165837 .

3. Диогенес, Ю. Кибербезопасность. стратегия атак и обороны / Ю. Диогенес, Э. Озкайя ; перевод с английского Д. А. Беликова. — Москва : ДМК Пресс, 2020. — 326 с. — ISBN 978-5-97060-709-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/131717

4. Мельников В.П., под ред., Куприянов А.И. Информационная безопасность : Учебник / .— Электрон. дан. — Москва : КноРус, 2021 .— 267 с. Internet access .— URL:https://www.book.ru/book/939292

5. Прохорова, О. В., Информационная безопасность и защита информации [Электронный ресурс] : учебник / Прохорова О. В. — 2-е изд., стер. — Санкт-Петербург : Лань, 2021 .— 124 с.—URL:https://e.lanbook.com/book/158939

6. Грибунин, В. Г. Комплексная система защиты информации на предприятии: учебное пособие для вузов / В. Г. Грибунин, В. В. Чудовский. – М.: Академия, 2009. – 411 с

7. Аверченков В. И. Организационная защита информации: учебное пособие для вузов 3-е изд., стер. - М.: Флинта, 2011. 224 с
8. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : [учебное пособие] / В. Ф. Шаньгин .— Москва : Форум : Инфра-М, 2011.
9. Васильев В.И. Интеллектуальные системы защиты информации: учебное пособие / В.И. Васильев. 3-е изд.,испр., и доп.- М.:№Издательство "Инновационное машиностроение", 2017. - 201 с..
10. Дуленко, В. А. Уголовно-правовые, криминологические и криминалистические проблемы расследования преступлений в сфере высоких технологий и компьютерной информации / В. А. Дуленко, Р. Р. Мамлеев, В. А. Пестриков ; ГОУ ВПО УГАТУ .— Уфа : УГАТУ, 2009 .— 214 с. : ил. ; 21 см .— Библиогр.: с. 206-213 .— ISBN 978-5-86911-979-7.
11. Малафеев, С. И. Надежность технических систем/ С. И. Малафеев, А. И. Копейкин .— Москва : Лань", 2016 .— 313 с.
12. Баданина Л.П. Основы общей психологии [Текст]: учебное пособие для вузов: рекомендовано Редакционно-издательским Советом Российской академии образования / Л.П. Баданина. – М.: Флинта, 2012. – 448 с.
13. Денисова О. П. Психология и педагогика: учеб.пособие: / О. П. Денисова; Рос.акад. образования, Моск. психол.-соц. ин-т - Москва: Флинта, 2013. - 236 с.
14. Карцева Л.В. Психология и педагогика социальной работы с семьей [Электронный ресурс]: учеб.пособие / Л.В. Карцева - Москва: Дашков и К, 2012. - 224 с.
15. Мандель Б.Р. Педагогика: / Мандель Б.Р. - Москва: ФЛИНТА, 2014.
16. Шарипов Ф.В. Педагогика и психология высшей школы: учебное пособие / Ф.В. Шарипов. - Москва: Логос, 2012. - 448 с.
17. Кузнецов И. Н. Основы научных исследований [Текст]: / И. Н. Кузнецов - Москва: Дашков и К, 2014 - 282 с.
18. Шкляр М. Ф. Основы научных исследований [Текст]: / М. Ф. Шкляр - Москва: Дашков и К, 2014 - 243 с.
19. Чулков В. А. Методология. Научных исследований: / Чулков В.А. - Москва: ПензГТУ (Пензенский государственный технологический университет), 2014.
20. Электронная библиотека диссертаций РГБ [Электронный ресурс]: Официальный сайт / Российская государственная библиотека - М.: РГБ, 2015.

Сроки проведения ГИА в соответствии с утвержденным графиком учебного процесса 3 курс, 5 семестр.

4. Проведение кандидатского экзамена для лиц с ОВЗ

Проведение кандидатского экзамена для обучающихся инвалидов и лиц с ОВЗ осуществляется с учетом рекомендованных условий обучения для инвалидов и лиц с ОВЗ. В таком случае требования к процедуре проведения и подготовке экзамена должны быть адаптированы под конкретные ограничения возможностей здоровья обучающегося, для чего должны быть предусмотрены специальные технические условия.