МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФГБОУ ВО «УФИМСКИЙ УНИВЕРСИТЕТ НАУКИ И ТЕХНОЛОГИЙ»

ИНСТИТУТ ИНФОРМАТИКИ МАТЕМАТИКИ И РОБОТОТЕХНИКИ

ПРИНЯТО
На заседании Ученого совета
Института информатики математики и робототехники
Протокол от «22» февраля 2024 г. № 4

Директор (декан) О.А.Кривошеева

УТВЕРЖДЕНО
Проректор по образовательной деятельности

И.А. Макаренко

м.п.

«11» марта 2024 г.

ПОДГОТОВКА КАДРОВ ВЫСШЕЙ КВАЛИФИКАЦИИ

ПРОГРАММА КАНДИДАТСКОГО ЭКЗАМЕНА ПО СПЕЦИАЛЬНОЙ ДИСЦИПЛИНЕ

НАУЧНАЯ СПЕЦИАЛЬНОСТЬ
2.3.6 Методы и системы защиты информации, информационная безопасность

Отрасль науки:
«Технические науки»

Уфа – 2024

Разработчик :

_____ / к.т.н. доцент кафедры ВТиЗИ, В.В. Сагитова

(подпись) (ученая степень, ученое звание, должность, фамилия и.о.)

Программа кандидатского экзамена по специальной дисциплине по научной специальности 2.3.6 Методы и системы защиты информации, информационная безопасность утверждена на заседании кафедры вычислительной техники и защиты информации (Протокол от «28» февраля 2024 г. № 6).

1. Общие положения

1.1. Область науки:
2. Технические науки
Группа научных специальностей:
2.3. Информационные технологии и телекоммуникации
Наименование отрасли науки, по которой присуждаются ученые степени:
Технические науки
Шифр научной специальности:
2.3.6. Методы и системы защиты информации, информационная безопасность

.2. Программа кандидатского экзамена по специальной дисциплине (далее «специальная дисциплина») по научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность разработана в соответствии с:

Федеральным законом от 29.12.2012 г. № 273-ФЗ «Об образовании в Российской Федерации»;

Постановлением Правительства РФ от 24.09.2013 г. № 842 «О порядке присуждения ученых степеней»;

Приказом Минобрнауки России от 28.03.2014 г. № 247 «Об утверждении Порядка прикрепления лиц для сдачи кандидатских экзаменов, сдачи кандидатских экзаменов и их перечня»;

Приказом Минобрнауки России от 05.08.2021 г. № 712 «О внесении изменений в некоторые приказы Министерства образования и науки Российской Федерации и Министерства науки и высшего образования Российской Федерации в сфере высшего образования и науки и признании утратившими силу приказов Министерства образования и науки Российской Федерации от 22 апреля 2013 г. № 296 и от 22 июня 2015 г. № 607»;

Приказом Министерства науки и высшего образования Российской Федерации от 24 февраля 2021 г. № 118 «Об утверждении номенклатуры научных специальностей, по которым присуждаются ученые степени, и внесении изменения в Положение о совете по защите диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук, утвержденное приказом Министерства образования и науки Российской Федерации от 10 ноября 2017 г. № 1093»;

Паспортом научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность;

Уставом УУНиТ;

Приказом УУНиТ от 07.03.2023 г. № 0527 «О Порядке прикрепления лиц для сдачи кандидатских экзаменов».

1.3. Программа кандидатского экзамена регламентирует цель, задачи, содержание, организацию кандидатского экзамена, порядок работы экзаменационной комиссии, порядок оценки уровня знаний соискателя ученой степени кандидата технических наук, и включает перечень вопросов, выносимых на кандидатский экзамен, рекомендации по подготовке к кандидатскому экзамену, в том числе, перечень литературы и ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для подготовки к кандидатскому экзамену.

1.4. Кандидатские экзамены представляют собой форму оценки степени подготовленности соискателя ученой степени кандидата технических наук (аспиранта/прикрепленного лица) к проведению научных исследований по конкретной научной специальности и отрасли науки, по которой подготавливается или подготовлена диссертация.

2. Цель проведения кандидатского экзамена

Целью проведения кандидатского экзамена по специальной дисциплине является оценка степени подготовленности соискателя ученой степени кандидата наук (аспиранта/прикрепленного лица) к проведению научных исследований по научной специальности 2.3.6 Методы и системы

защиты информации, информационная безопасность и отрасли науки технические науки, по которой подготавливается или подготовлена диссертация:

– проверка сформированности умений в области применения методов и систем защиты информации, использования междисциплинарных установок и общенаучных понятий в решении комплексных задач теории и практики в конкретно научной исследовательской деятельности;

– владение основными понятиями и методами обеспечения информационной безопасности на уровне, позволяющем получать качественные результаты при решении теоретических и прикладных задач в области изучаемых дисциплин;

– получение практических навыков аргументации в обосновании научного статуса и актуальности конкретной исследовательской задачи, в работе с внеэмпирическими методами оценки выдвигаемых проблем и гипотез.

Сдача кандидатских экзаменов обязательна для присуждения ученой степени кандидата наук.

3. Задачи, решаемые в ходе сдачи кандидатского экзамена

В ходе сдачи кандидатского экзамена необходимо оценить:

– способность к критическому анализу и оценке современных научных достижений, генерированию новых идей при решении исследовательских и практических задач, в том числе в междисциплинарных областях;

– способность проектировать и осуществлять комплексные исследования, в том числе междисциплинарные, на основе целостного системного научного мировоззрения с использованием знаний в области методов и систем защиты информации, информационной безопасности.

4. Структура и содержание кандидатского экзамена

4.1. Кандидатский экзамен по специальной дисциплине по научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность проводится в устной форме по билетам (Приложение № 1). Экзаменационный билет включает в себя три теоретических вопроса, два вопроса, непосредственно связанных с темой и разработками диссертационной работы в области математического и программного обеспечения вычислительных машин, комплексов и компьютерных сетей.

Продолжительность устного ответа на экзамене – 20 минут, время на подготовку к ответу на экзаменационный билет – до 30 минут.

4.2. Комиссия по приему кандидатского экзамена по специальной дисциплине правомочна принимать кандидатский экзамен по специальной дисциплине, если в ее заседании участвуют не менее 3 специалистов, имеющих ученую степень кандидата или доктора наук по научной специальности, соответствующей специальной дисциплине, в том числе 1 доктор наук.

Решение, принятое комиссией, оформляется протоколом по установленной Университетом форме.

4.3. Университет вправе применять дистанционные образовательные технологии при проведении кандидатского экзамена. Особенности проведения кандидатских экзаменов с применением дистанционных образовательных технологий определяются локальным нормативным актом Университета.

При проведении кандидатского экзамена с применением дистанционных образовательных технологий Университет обеспечивает идентификацию личности аспирантов/прикрепленных лиц и контроль соблюдения требований, установленных локальным нормативным актом.

5. Перечень тем, вынесенных на кандидатский экзамен

Тема 1. Нормативно-правовые основы защиты информации

Тема 2. Теория информационной безопасности и методология защиты информации

Тема 3. Организационная защита информации

Тема 4. Инженерно-техническая защита информации

Тема 5. Программно-аппаратная защита информации

6. Перечень документов и материалов, которыми разрешается пользоваться на кандидатском экзамене

Программа кандидатского экзамена по специальной дисциплине по научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Во время проведения кандидатского экзамена аспирантам/прикрепленным лицам, привлекаемым к его проведению, запрещается иметь при себе и использовать средства связи.

7. Перечень вопросов для проведения кандидатского экзамена:

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.

8. Порядок оценки уровня знаний соискателя ученой степени кандидата наук

8.1. Оценка уровня знаний соискателя ученой степени кандидата наук определяется экзаменационными комиссиями по пятибалльной системе: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

8.2. При оценке знаний и уровня подготовки соискателя ученой степени кандидата наук, определяется:

– уровень освоения материала, предусмотренного программой кандидатского экзамена;
– умение использовать теоретические знания при выполнении практических задач;

– обоснованность, четкость, краткость изложения ответа.

8.3. Общими критериями, определяющими оценку уровня знаний соискателя ученой степени кандидата наук, являются:

– для оценки «отлично»: наличие глубоких и исчерпывающих знаний в объеме пройденного программного материала, правильные и уверенные действия по применению полученных знаний на практике, грамотное и логически стройное изложение материала при ответе, знание дополнительно рекомендованной литературы;

– для оценки «хорошо»: наличие твердых и достаточно полных знаний программного материала, незначительные ошибки при освещении заданных вопросов, правильные действия по применению знаний на практике, четкое изложение материала;

– для оценки «удовлетворительно»: наличие твердых знаний пройденного материала, изложение ответов с ошибками, уверенно исправляемыми после дополнительных вопросов, необходимость наводящих вопросов, правильные действия по применению знаний на практике;

– для оценки «неудовлетворительно»: наличие грубых ошибок в ответе, непонимание сущности излагаемого вопроса, неумение применять знания на практике, неуверенность и неточность ответов на дополнительные и наводящие вопросы.

9. Методические указания по подготовке к сдаче кандидатского экзамена

При подготовке к кандидатскому экзамену рекомендуется:

Внимательно прочесть источники в списке рекомендуемой литературы и проанализировать информацию.

Сделать выписки (конспект) необходимой информации в соответствии с темами и экзаменационными вопросами.

Систематизировать и классифицировать полученные данные по тематическим разделам и экзаменационным вопросам.

Составить рабочие записи – ключевые опорные пункты в соответствии с логикой ответа на экзаменационные вопросы.

Подобрать необходимую иллюстративную информацию по содержанию ответа на экзаменационные вопросы.

В ходе подготовки к выполнению практического задания обучающийся анализирует результаты диссертационного исследования.

10. Перечень рекомендуемой литературы и ресурсов информационно-телекоммуникационной сети «Интернет»

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.

Приложение № 1

Билет 1

0. Законодательные и правовые основы защиты компьютерной информации информационных технологий.
1. Типы несанкционированного доступа и условия работы средств защиты.
2. Способы встраивания защитных механизмов в программное обеспечение.