РАЗРАБОТАНА

Кафедрой информационной безопасности и цифровых технологий

03.02.2022, протокол № 7

УТВЕРЖДЕНА

Ученым советом факультета цифровых технологий и кибербезопасности

10.02.2022, протокол № 22

ПРОГРАММА ВСТУПИТЕЛЬНОГО ИСПЫТАНИЯ

для поступающих на обучение по образовательным программам высшего образования – программам подготовки научных и научно-педагогических кадров в аспирантуре в 2022 году

Научная специальность
2.3.6 Методы и системы защиты информации, информационная безопасность

Астрахань – 2022 г.

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Цель программы: подготовка высококвалифицированных специалистов, обладающих креативным мышлением и навыками научно-исследовательской работы для создания и использования новых прогрессивных подходов к методам и системам защиты информации, информационной безопасности, способных решать задачи, связанные с использованием наукоемких информационных технологий.

Лица, желающие освоить научную специальность 2.3.6 Методы и системы защиты информации, информационная безопасность, должны иметь высшее профессиональное образование (специалитет или магистратуру).

Лица, имеющие высшее профессиональное образование (специалитет или магистратуру), принимаются в аспирантуру по результатам сдачи вступительных экзаменов на конкурсной основе по программа вступительных испытаний в аспирантуру.

Библиографический список (основная литература)

1. Доктрина информационной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. №646.
2. Крылов Г.О., Никитина В.Л. Понятийный аппарат информационной безопасности финансово-экономических систем. Энциклопедический словарь - М.: Финансовый университет, 2016.
3. Платонов В.В. Программно-аппаратные средства защиты информации: учебник для вузов. - М.: Издательский центр «Академия», 2013.
4. Сердюк В.А. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий: учебное пособие. - М.: Высшая школа экономики, 2011.
5. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. - М.: ДМК Пресс, 2012.
6. Фомичёв, В.М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты: учебник для академического бакалавриата / В. М. Фомичёв, Д. А. Мельников; под ред. В. М. Фомичёва. — М.: Юрайт, 2017.
7. 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; под ред. В. М. Фомичёва. — М.: Юрайт, 2016.
8. Актуальные проблемы информационного права. Учебник для вузов. ФГОС 3+. В.И. Авдийский, Г.О. Крылов и др.; под ред. И.Л. Бачило, М.А. Лапиной, М.: JUSTITIA, 2016.

Основные критерии оценивания ответа поступающего в аспирантуру

Критерии	Уровни и подуровни знаний	Балл
Критерий 1.	Ответ полный, без замечаний, хорошо структурированный, продемонстрировано хорошее знание теоретических подходов к анализу и решению рассматриваемой проблемы, проиллюстрировано примерами, даны аргументированные,	5

	полные и логичные ответы на вопросы членов комиссии, проявлено творческое отношение к предмету.	
Критерий 2.	Ответ полный с незначительными замечаниями, недостаточно структурирован, продемонстрировано знание основных теоретических подходов к анализу и решению рассматриваемой проблемы, проиллюстрировано примерами, ответы на вопросы членов комиссии даны с незначительными замечаниями.	4
Критерий 3.	В ответе есть упущения, ответ недостаточно структурирован, знание основных теоретических подходов к анализу и решению рассматриваемой проблемы продемонстрировано с упущениями, есть затруднения при практическом применении теории, есть затруднения при ответе на вопросы комиссии.	3
Критерий 4.	В ответе есть значительные упущения и неточности, многие основные положения теоретических подходов к анализу и решению рассматриваемой проблемы не представлены или в их выводе допущены ошибки, ответ не структурирован, ответы на вопросы комиссии отсутствуют.	2

Перечень вопросов к вступительному испытанию

Основные понятия и принципы теории информационной безопасности

1. Угрозы информационной безопасности.
2. Виды информации, методы и средства обеспечения информационной безопасности.
3. Методы нарушения конфиденциальности, целостности и доступности информации.
4. Основы комплексного обеспечения информационной безопасности.
5. Модели, стратегии и системы обеспечения информационной безопасности.
6. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем.
7. Лицензирование и сертификация в области защиты информации.
8. Правовые основы защиты информации.
9. Организационные основы защиты информации.

Организация ЭВМ и вычислительных сетей

1. Локальные и глобальные вычислительные сети, типовые конфигурации, маршрутизация.
2. Основные протоколы обмена данными в вычислительных сетях.
3. Системы управления базами данных, реляционная, иерархическая и сетевая модели, распределенные БД.
4. Деревья и графы, их представление в ЭВМ, обходы графов.
5. Алгоритмы на графах, выделение компонент связности.
6. Кратчайшие пути в графе, минимальный остов графа.
7. Задача сортировки и основные алгоритмы сортировки.
8. Поиск информации методом хеширования.

9. Контрольно-испытательные и логико- аналитические методы анализа безопасности программ.
10. Методы и средства хранения ключевой информации в ЭВМ.
11. Защита программ от изучения, защита от изменения, контроль целостности.
12. Защита от разрушающих программных воздействий.

Криптографическая защита информации

1. Шифры замены и перестановки, их свойства, композиции шифров.
2. Криптостойкость шифров, основные требования к шифрам.
3. Теоретическая стойкость шифров, совершенные и идеальные шифры.
4. Блоковые шифры.
5. Потоковые шифры.
6. Криптографические хеш-функции, их свойства и использование в криптографии.
7. Методы получения случайных последовательностей, их использование в криптографии.
8. Системы шифрования с открытыми ключами.
9. Криптографические протоколы.
10. Протоколы распределения ключей.
11. Протоколы идентификации.
12. Парольные системы разграничения доступа.
13. Цифровая подпись.
14. Стойкость систем с открытыми ключами

Методы математического моделирования

1. Методы решения систем линейных уравнений.
2. Методы интерполяции.
3. Методы численного интегрирования.
4. Методы численного решения дифференциальных уравнений.
5. Численные методы нахождения экстремумов функций.
6. Элементы комбинаторики: перестановки, выборки, сочетания и размещения без повторений.
7. Сочетания и размещения с повторениями, биномиальные коэффициенты, их свойства.
8. Алгебра логики, формулы алгебры логики, высказывания и операции, построение формул.
9. Случайные величины, математическое ожидание и дисперсия.
10.Основные законы распределения случайной величины.
11. Центральная предельная теорема.
12. Цепи Маркова.
13.Система массового обслуживания без очереди и с очередью.

Методы и средства технической защиты информации

1. Структура, классификация и основные характеристики технических каналов утечки информации.
2. Побочные электромагнитные излучения и наводки.
3. Классификация средств технической разведки, их возможности.
4. Концепция и методы инженерно-технической защиты информации.
5. Методы скрытия речевой информации в каналах связи.

6. Методы обнаружения и локализации закладных устройств.
7. Методы подавления опасных сигналов акустоэлектрических преобразователей.
8. Методы подавления информативных сигналов в цепях заземления и электропитания.
9. Виды контроля эффективности защиты информации.
10. Методы расчета и инструментального контроля показателей защиты информации.
11. Утечка информации от вспомогательной аппаратуры и кабелей, проходящих через помещение.
12. Несанкционированный съем информации с помощью радиозакладок.
13. Основные характеристики радиозакладок.
14. Прослушивание информации от пассивных закладок.
15. Приемники информации с радиозакладок.
16. Деконспирационные признаки радиозакладок.
17. Методы пассивной защиты от утечки по электромагнитному каналу.
18. Технические средства для поиска работающих радиозакладок.
19. Поиск радиозакладок нелинейными радиолокаторами.
20. Нелинейные радиолокаторы с непрерывным режимом работы.
21. Нелинейные радиолокаторы с импульсным режимом работы.
22. Основы радиоэлектронной борьбы (РЭБ).
23. Основы информационного противоборства.
24. Проблемы деанонимизации в теневом интернете.
25. Использование распределенных реестров и технологии блокчейн в задачах информационной безопасности.

Содержание программы

1. Избранные разделы математики и информатики.

1. Информация, сообщения, информационные системы и процессы как объекты информационной безопасности.
2. Основные свойства информации. Мера количества информации. Энтропия.
3. Случайные события. Полная группа событий. Зависимые и независимые случайные события. Вероятность случайного события.
4. Условная вероятность. Формула полной вероятности. Теорема Байеса.
5. Случайные величины и их характеристики: функция распределения, моменты, характеристические функции.
6. дискретные и непрерывные случайные величины. Биноминальный закон распределения. Нормальный закон распределения. Центральная предельная теорема Ляпунова.
7. Основные задачи математической статистики: точечная оценка, построение доверительного интервала, различение статических гипотез.
8. Сетевая модель OSI/ISO. Уровни модели OSI.
9. Сетевая модель OSI/ISO. Примеры протоколов.

2. Теоретические основы информационной безопасности

1. Понятие угрозы информационной безопасности. Виды угроз.

2. Основные методы реализации угроз информационной безопасности. Основные принципы обеспечения информационной безопасности (ИБ) в автоматизированных системах (АС).
3. Методы оценки угроз ИБ. Модель угроз.
4. Причины, виды и каналы утечки информации.
5. Построение систем защиты от угрозы нарушения конфиденциальности информации.
6. Построение систем защиты от угрозы нарушения целостности информации.
7. Построение систем защиты от угрозы отказа доступа к информации.
8. Политика безопасности. Понятие политики безопасности. Понятия доступа и монитора безопасности. Основные типы политики безопасности.
9. Модели безопасности. Модель матрицы доступов HRU.
10. Модель распространения прав доступа Take-Grant.
11. Модель системы безопасности Белла-Лападула.
12. Основные критерии защищенности АС. Классификация систем защиты АС. Руководящие документы Государственной технической комиссии России.
13. Общие критерии (ОК). Основные положении ОК.

3. Основы криптографической защиты информации.

1. Криптографические методы зашиты информации. Основные понятия криптографии. Исторические шифры.
2. Теоретическая, практическая и временная стойкость системы криптографической защиты.
3. Методы получения псевдослучайных последовательностей. Современные поточные и блочные алгоритмы шифрования.
4. Системы симметричного шифрования.
5. Системы асимметричного шифрования, открытый ключ, электронная подпись.
6.Вопросы генерации и распределения ключей. Обоснование стойкости криптографической защиты.

Рекомендуемая дополнительная литература

1. Родичев Ю.А. Нормативная база и стандарты в области информационной безопасности. Учебное пособие. Стандарт третьего поколения. Учебник для вузов - Спб: Питер, 2017.
2. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности: учебное пособие для вузов. - М.: Горячая линиятелеком, 2006.
3. Гатчин Ю.А., Климова Е.В. Основы информационной безопасности - Спб: СПбГУ ИТМО, 2009.
4. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. Технические средства и методы защиты информации: учебник для вузов. - М.: Машиностроение, 2009.
5. Ленков С.В., Перегудов Д.А. Методы и средства защиты информации.В 2-х томах. - М.: Арий, 2009.
6. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства. - М.: ДМК Пресс, 2008.
7. Сычев Ю.Н. Основы информационной безопасности. - М.: Евразийский открытый институт, 2010.

8. Крылов Г.О., Ларионова С.Л., Никитина В.Л. Базовые понятия информационной безопасности. Учебное пособие. - М.: РУСАЙНС, 2016. Ларичев О.И. Теория и методы принятия решений. М.: Логос, 2000.