Перечень вопросов вступительных испытаний

Группа научных специальностей	1.2. Компьютерные науки и информатика
Научная специальность	1.2.4. Кибербезопасность
Кафедра	интеллектуальных систем и защиты информации

1. Анализ известных и вновь выявляемых уязвимостей, их систематизация,
2. Разработка методов интеллектуального поиска новых классов уязвимостей.
3. Моделирование политик информационной безопасности, угроз и атак.
4. Методические основы разработки профилей защиты.
5. Методы проектирования, моделирования, анализа, трансформации программ для выявления потенциальных уязвимостей в программных системах с учетом специфики фаз жизненного цикла.
6. Разработки требований, проектирования архитектуры, разработки программного кода, тестирования, верификации, сертификации и эксплуатации.
7. Методы, алгоритмы и средства пострелизного глубокого анализа защищенности программно-аппаратного обеспечения.
8. Методы интеграции средств защиты на уровне аппаратуры и на уровне программного обеспечения.
9. Методы, алгоритмы и средства обеспечения устойчивого функционирования программно-аппаратных систем в условиях злонамеренного воздействия
10. Методы обфускации и безопасной компиляции программ.
11. Интеллектуальный масштабируемый мониторинг инцидентов безопасности в распределенных программно-аппаратных системах.
12. Методы оперативного реагирования на выявленные угрозы.
13. Масштабируемые средства интеллектуального анализа данных и процессов в распределенных системах, включая социальные сети.
14. Разработка методических основ для создания и развития метрик оценки защищенности,
15. Разработка уровня доверия компьютерных систем и стандартов в области кибербезопасности.
16. Системы и языки программирования.
17. Машинно-ориентированные, проблемноориентированные и универсальные языки. Алфавит, синтаксис и семантика.
18. Способы описания языков программирования. Трансляция.
19. Типы данных, способы задания типа. Константы и переменные. Идентификаторы.

20. Структурированные типы данных. Выражения, операции, операторы.
21. Арифметические и логические операции и операторы. Программирование ввода и вывода информации.
22. Подпрограммы, методы передачи параметров при использовании подпрограмм. Основы объектно-ориентированного программирования. Инкапсуляция, наследование, полиморфизм.
23. Шифры замены и перестановки, их свойства, композиции шифров. Криптостойкость шифров, основные требования к шифрам.
24. Теоретическая стойкость шифров, совершенные и идеальные шифры.
25. Блоковые шифры. Потоковые шифры.
26. Криптографические хеш-функции, их свойства и использование в криптографии.
27. Методы получения случайных последовательностей, их использование в криптографии.
28. Системы шифрования с открытыми ключами. Криптографические протоколы.
29. Протоколы распределения ключей. Протоколы идентификации.
30. Парольные системы разграничения доступа. Цифровая подпись. Стойкость систем с открытыми ключами

Список рекомендуемой литературы:

1. Сердюк В.А. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий: учебное пособие. - М.: Высшая школа экономики, 2017. – 252с.
2. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. - М.: ДМК Пресс, 2019. – 325с.
3. 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. – 564с.
4. 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, 2018. – 346с.
5. 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, 2017.