МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего профессионального образования
«Санкт-Петербургский государственный университет аэрокосмического приборостроения»

Центр организационно-методического обеспечения магистерской подготовки

«УТВЕРЖДАЮ»
Ректор ГУАП
_____Ю.А. Антохина
«13» 04 2015

ПРОГРАММА ВСТУПИТЕЛЬНЫХ ИСПЫТАНИЙ ПО ПРИЕМУ В МАГИСТРАТУРУ НА НАПРАВЛЕНИЕ ПОДГОТОВКИ

10.04.01 «Информационная безопасность»

Санкт-Петербург 2015

Рассмотрено и рекомендовано к использованию на заседании
Координационного совета по магистерской подготовке в ГУАП
09.04.2015 протокол № 04/КС

Программа согласована с выпускающей кафедрой;

Ответственный за ОП 10.04.01 кафедры № 51
профессор, д.т.н., зав. каф. № 51 _____ Е.А. Крук

Программа соответствует федеральному государственному образовательному стандарту высшего образования по направлению 10.04.01

Директор ЦОМОМП _____ Е.Г.Семенова

1 ОБЩИЕ ПОЛОЖЕНИЯ ПО ПРОВЕДЕНИЮ ВСТУПИТЕЛЬНЫХ ИСПЫТАНИЙ ПО ПРИЕМУ В МАГИСТРАТУРУ НА НАПРАВЛЕНИЕ 10.04.01 «Информационная безопасность»

1.1 Настоящая Программа, составленная в соответствии с федеральнымм государственнымм образовательнымм стандартом ВО по направлению 10.04.01 «Информационная безопасность», устанавливает содержание вступительных испытаний с целью определения подготовленности претендентов и наличия способностей для продолжения образования в магистратуре по направлению 10.04.01.

1.2 В качестве вступительного испытания для претендентов на обучение в магистратуре ГУАП в соответствии с СТО ГУАП. СМКО 2.72 - «Магистерская подготовка в ГУАП», установлен междисциплинарный экзамен, проводимый в письменной или устной форме.

1.3 Решение экзаменационной комиссии заносится в протокол.

2 ПРОГРАММА ДЛЯ ПРОВЕДЕНИЯ ВСТУПИТЕЛЬНЫХ ИСПЫТАНИЙ

2.1 Программа вступительного испытания, содержит вопросы в объеме требований, предъявляемых образовательным стандартом высшего профессионального образования уровня подготовки бакалавра по направлению, соответствующему направлению магистратуры.

2.2 Конечной целью вступительного испытания является определение уровня знаний и компетенций абитуриента по 100-балльной шкале.

Основное вступительное испытание предназначено для определения степени подготовленности абитуриента к обучению по выбранному направлению магистерской подготовки, для определения уровня его знаний и компетенций. По результатам основного вступительного испытания приемная комиссия определяет проходной балл для зачисления абитуриентов на данное направление магистерской подготовки.

Целью предварительного вступительного испытания является определение степени подготовленности абитуриента к обучению по выбранному направлению магистерской подготовки, владение им основными понятиями и терминологией в данной области. Экзаменационная комиссия выставляет претенденту оценку по 100-балльной шкале. Успешно прошедшими предварительное вступительное испытание считаются лица, набравшие не менее 60 баллов. При наборе меньшего числа баллов абитуриент не допускается к прохождению основного вступительного испытания.

Рекомендуется следующая система оценивания результатов предварительного вступительного испытания по следующей 100-балльной квантованной шкале:

- 100 баллов - в ответе отражены основные концепции и теории по данному вопросу, проведен их критический анализ и сопоставление, описанные теоретические положения иллюстрируются практическими примерами и экспериментальными данными. Абитуриентом формулируется и обосновывается собственная точка зрения на заявленные проблемы, материал излагается профессиональным языком с использованием соответствующей системы понятий и терминов.
- 80 баллов - в ответе описываются и сравниваются основные современные концепции и теории по данному вопросу, описанные теоретические положения иллюстрируются практическими примерами, абитуриентом формулируется собственная точка зрения на заявленные проблемы, однако он испытывает затруднения в ее аргументации. Материал излагается профессиональным языком с использованием соответствующей системы понятий и терминов.
- 60 баллов - в ответе отражены лишь некоторые современные концепции и теории по данному вопросу, анализ и сопоставление этих теорий не проводится. Абитуриент испытывает значительные затруднения при иллюстрации теоретических положений практическими примерами. У абитуриента отсутствует собственная точка зрения на заявленные проблемы.

Материал излагается профессиональным языком с использованием соответствующей системы понятий и терминов.

– 40 баллов - ответ не отражает современные концепции и теории по данному вопросу. Абитуриент не может привести практических примеров. При изложении материала не используются понятия и термины соответствующей научной области.

3 ПЕРЕЧЕНЬ ВОПРОСОВ ДЛЯ ПРОВЕДЕНИЯ ВСТУПИТЕЛЬНЫХ ИСПЫТАНИЙ

3.1 Перечень вопросов для проведения предварительного вступительного испытания

1. Алгоритмы: свойства и правила составления.
2. Рекурсивные алгоритмы.
3. Метод декомпозиции.
4. Эвристические алгоритмы.
5. Этапы построения алгоритмов.
6. Метод производящих функций как средство решения рекуррентных уравнений.
7. Решение задач с помощью поиска по дереву.
8. Динамическое программирование как метод проведения исчерпывающего поиска.
9. Метод ветвей и границ как метод исчерпывающего поиска.
10. Вычисление нижних и верхних границ при решении задачи коммивояжера методом ветвей и границ.
11. Методы решета.
12. Сортировка простыми вставками.
13. Среднее число беспорядков в перестановке.
14. Сортировка Шелла.
15. Пузырьковая сортировка.
16. Быстрая сортировка.
17. Анализ сложности быстрой сортировки.
18. Сортировки выбором. Турниры.
19. Пирамидальная сортировка. Сложность пирамидальной сортировки.
20. Вычисление порядковых статистик. Сложность вычисления порядковых статистик.
21. Сортировка распределением.
22. Внешняя сортировка. Сортировка слиянием.
23. Задача о расписании для системы параллельных процессоров.
24. Задача о минимизации сложности умножения матриц.
25. Методы задания графов.
26. Поиск в глубину (на графе). Сложность поиска в глубину.
27. Классификация методов сортировки.
28. Вирусы, "черви" и "троянские кони".
29. Симметричные шифры. Свойства, принципы построения.
30. Асимметричные шифры. Свойства, принципы построения.
31. Парольные системы защиты от несанкционированного доступа к информации, принципы их построения.
32. Криптография и труднорешаемые задачи.
33. Политика безопасности. Основные понятия и определения.
34. Понятие класса алгоритмов.
35. Оценка сложности решения задачи о фальшивой монете.
36. Схемы аутентификации (основные принципы).
37. Детерминированная машина Тьюринга и класс задач P.
38. Недетерминированные алгоритмы и класс задач NP.
39. Полиномиальная эквивалентность и NP-полные задачи.
40. Задача выполнимости. Теорема Кука.
41. Основные NP- полные задачи.
42. Этапы построения модели системы.

43. Построение имитационной модели. Выбор параметров.
44. Понятие кибернетической модели.
45. Задачи планирования эксперимента.
46. Защищенные соединения в Internet.
47. Понятие кода, исправляющего ошибки. Границы мощности кода.
48. Задача обеспечения аутентификации. Цифровая подпись.
49. Задачи информационной безопасности. Понятия конфиденциальности, подлинности и целостности информации.
50. Обобщенная структура канала передачи информации. Составные элементы модели канала.

3.2 Перечень вопросов для проведения основного вступительного испытания

1. Задача комплексной оценки защищенности системы.
2. Причины, виды и каналы утечки информации ТКС.
3. Функциональное описание аппаратной реализации прямого и обратного преобразований для режима шифрования CFB. Свойства этого режима.
4. Функциональное описание аппаратной реализации прямого и обратного преобразований для режима шифрования OFB. Свойства этого режима.
5. Алгоритм шифрования с управляемыми перестановками.
6. Алгоритм шифрования с управляемыми подстановками.
7. Алгоритм хэширования по ГОСТ Р3411-94.
8. М-последовательности; их основные свойства и методы генерации.
9. Функции Уолша; их свойства и применение в системах связи с кодовым разделением каналов (CDMA).
10. Шифр DES.
11. Шифр ГОСТ 28147-89.
12. Шифр AES.
13. Система RSA.
14. Распределение ключей. Протокол Диффи-Хеллмана.
15. Система Меркли-Хеллмана.
16. Задача обеспечения аутентификации. Цифровая подпись.
17. Подпись RSA.
18. Подпись Эль-Гамаля.
19. Подпись ГОСТ Р 34.10-01.
20. Слепая подпись.
21. Определение линейной сложности потокового шифра. Алгоритм Евклида.
22. Криптографические хэш-функции. Основные свойства. MDC, MAC.
23. Квантовая криптография. Основные принципы и свойства.
24. Суперпозиция нескольких регистров сдвига. Определение линейной сложности и периода схем построенных на суперпозиции регистров сдвига.
25. Шифры гаммирования. Основные схемы образования.
26. Сертификаты открытых ключей.
27. Видеонаблюдение. Телевизионный сигнал и его параметры. Визуальное определение качества изображения.
28. Съем информации с проводных устройств и способы его обнаружения и устранения.
29. Принципы действия и особенности конструкций печатающих устройств, позволяющие их идентифицировать.
30. Показатели защищенности средств вычислительной техники от НСД (по материалам ГосТехКомиссии).
31. Порядок обследования помещений в целях проверки их информационной безопасности.
32. Модель атака/уязвимость/актив/ ущерб и ее составляющие.

33. Охрана коммерческой тайны. Организация конфиденциального делопроизводства.
34. Закон о техническом регулировании. Сертификация и лицензирование в безопасности.
35. Закон о техническом регулировании. Стандартизация и стандарты в безопасности.
36. Интеллектуальная собственность, Авторское право.
37. Проприетарное и свободное ПО с точки зрения информационной безопасности.
38. Коммерческая разведка и контрразведка.
39. Закон о персональных данных и мероприятия по исполнению его требований.
40. Социальная инженерия и защита от нее.
41. Закон о рекламе, закон о средствах массовой информации и вопросы информационной безопасности.
42. Потоковые шифры. Свойства, принципы построения.
43. Примеры потоковых шифров. Шифр Вернама, генератор Геффе, шифр А5.
44. Построение профиля линейной сложности. Алгоритм Берлекэмпа-Месси.
45. Система Мак-Элиса.
46. Пороговое разделение секрета.
47. Доказательства с нулевым разглашением.
48. Протокол идентификации Фиата-Шамира.
49. Основные принципы дифференциального криптоанализа.
50. ISO 17799 Политика безопасности.
51. ISO 17799 Безопасность приложений (программный продукт).
52. ISO 17799 Безопасность системных файлов.
53. ISO 17799 Защита от вредоносного программного обеспечения.
54. ISO 17799 Управление доступом пользователя.
55. ISO 17799 Контроль доступа в операционную систему.
56. ISO 17799 Безопасность носителей данных.
57. Электронные деньги.
58. Идентификация. Системы с нулевым разглашением.
59. Атаки на системы с открытым ключом (по выбору).
60. Атаки на цифровые подписи (по выбору).
61. Передача и хранение паролей.
62. Защита информации на уровне ее содержания (стеганография).
63. Модель контроля целостности Кларка-Вилсона.
64. Основные типы политики безопасности.
65. Модель матрицы доступа HRU.
66. Модель прав доступа TAKE-GRANT.
67. Модель безопасности Белла-Лападула.
68. Защита от угрозы раскрытия параметров информационной системы.
69. Требования к выбору пароля.
70. Классификация возможных угроз информационной безопасности.
71. Методы реализации угроз информационной безопасности на различных уровнях доступа к информации в автоматизированных системах.
72. Основные принципы обеспечения информационной безопасности в автоматизированных системах.
73. Протоколы безопасности сетевой ОС Unix.
74. Протокол HTTP.
75. Постановка задачи кодирования канала. Пропускная способность канала связи.
76. Постановка задачи помехоустойчивого кодирования.
77. Правила безопасности электронной почты.
78. Организация работ по обеспечению безопасности информации на предприятии.
79. Правила разработки программного обеспечения.
80. Способы оценки угроз безопасности информации и расходов на техническую защиту.
81. Виды информации, защищаемой техническими средствами.
82. Демаскирующие признаки объектов защиты.
83. Источники и носители информации, защищаемой техническими средствами.

84. Принципы записи и съема информации с носителей.
85. Виды угроз безопасности информации, защищаемой техническими средствами.
86. Принципы добывания и обработки информации техническими средствами.
87. Классификация и структура технических каналов утечки информации.
88. Основные способы и принципы работы средств наблюдения объектов, подслушивания и перехвата сигналов.
89. Системный подход к инженерно-технической защите информации.
90. Основные этапы проектирования системы защиты информации техническими средствами.
91. Принципы моделирования объектов защиты и технических каналов утечки информации.
92. Способы и принципы работы средств защиты информации от наблюдения, подслушивания и перехвата.
93. Организационные и технические меры инженерно-технической защиты информации в государственных и коммерческих структурах.
94. Контроль эффективности защиты информации.
95. Классификация методов доступа к информационным ресурсам.
96. Одно- и многофакторная аутентификация.
97. Принципы работы биометрической системы аутентификации.
98. Протоколы аутентификации.
99. Организация пропускного режима на предприятии.
100. OTP-токены. Методы доступа с применением OTP-токенов.