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

«УТВЕРЖДАЮ»
Ректор ГУАП
_____ Ю.А. Антохина
«21» 09 2017

ПРОГРАММА ВСТУПИТЕЛЬНОГО ИСПЫТАНИЯ ПРИ ПРИЕМЕ НА ОБУЧЕНИЕ ПО ПРОГРАММЕ МАГИСТРАТУРЫ НА НАПРАВЛЕНИЕ ПОДГОТОВКИ

10.04.01 Информационная безопасность

Санкт-Петербург 2017

Программа вступительных испытаний в магистратуру по направлению 10.04.01 Информационная безопасность

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 вбезопасности.
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 дифференциальногокриптоанализа.
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.

Критерии оценивания вступительного испытания в магистратуру.

Экзаменационное задание содержит три теоретических вопроса в соответствии с Программами вступительных испытаний по соответствующим направления подготовки. При проверке каждый из трех вопросов оценивается по тридцатитрехбалльной системе оценивания в зависимости от полноты и правильности выполнения задания. Каждая фактическая ошибка снижает оценку на 3 балла, если ошибка является не существенной, то оценка снижается на 1-2 балла в зависимости от ошибки. Полнота ответа является существенным условием для выставления максимального балла. Неполные ответы оцениваются в процентном отношении к полному ответу. Исходя из процента полноты ответа и количества ошибок выставляется балл за каждый из трех вопросов. Дополнительно оценивается в один балл или ноль баллов общее впечатление от работы – грамотность ответов и четкость формулировок.