МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное
учреждение высшего образования
«ЮЖНЫЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Программа утверждена на заседании
Ученого совета Института
компьютерных технологий и
информационной безопасности
«12» апреля 2022 г., протокол № 4

УТВЕРЖДАЮ
Директор Института
компьютерных технологий и
информационной безопасности
_____ Г.Е. Веселов
«12» _____2022 г.

Программа вступительного испытания по Методам и системам защиты информации, информационной безопасности

Форма обучения: очная

г. Ростов-на-Дону
г. Таганрог
2022

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Вступительное испытание «Методы и системы защиты информации, информационной безопасности» по образовательной программе высшего образования – программе подготовки научных и научно-педагогических кадров в аспирантуре, соответствующей научной специальности 2.3.6. Методы и системы защиты информации, информационной безопасности, проводится в соответствии с регламентирующими документами Министерства науки и высшего образования Российской Федерации и локальными нормативными актами Южного федерального университета (ЮФУ).

Вступительное испытание проводится в соответствии с утверждённым расписанием. Протокол сдачи вступительного испытания подписывается членами экзаменационной комиссии. В состав экзаменационной комиссии, утверждаемой приказом ректора ЮФУ, включаются ведущие учёные ЮФУ, проводящие научно-исследовательскую деятельность в соответствующей научной области.

Вступительное испытание проводится по экзаменационным билетам, составленным по приведённой ниже вопросам. Каждый экзаменационный билет содержит два вопроса. Поступающий готовит ответы на вопросы в письменной форме, а перед комиссией даёт ответы на вопросы экзаменационного билета в форме собеседования.

Программа вступительного испытания содержит также библиографические описания источников информации, рекомендуемых для подготовки к вступительному испытанию.

ВОПРОСЫ ВСТУПИТЕЛЬНОГО ИСПЫТАНИЯ

1. Персональные данные о гражданах; права на доступ к информации
2. Проблемы построения информационного общества
3. Понятие сертификата открытого ключа. Принципы работы удостоверяющих центров.
4. Защищенная информационная система и система защиты информации;
5. Доктрина информационной безопасности РФ. Методы обеспечения информационной безопасности РФ в различных сферах.
6. Мандатный доступ. Правила управления доступом.
7. Политика безопасности организации
8. Сравнение Доктрин информационной безопасности РФ 2000 года и 2016 года.
9. Аудит. Цели и этапы аудита безопасности
10. Применение симметричных криптосистем для защиты компьютерной информации в информационных системах. Американский стандарт шифрования данных DES; основные режимы работы алгоритма DES.
11. Основные положения государственной политики обеспечения информационной безопасности РФ.
12. Дезинформация и борьба с нею. Привести примеры.
13. Отечественный стандарт шифрования данных; режим простой замены; режим гаммирования; режим гаммирования с обратной связью; режим выработки имитовставки; блочные и поточные шифры.
14. Гуманитарные аспекты защиты информации.
15. Защита русского языка – важное условие информационной безопасности России.
16. Методы идентификации и проверки подлинности пользователей компьютерных систем. Основные понятия и концепции; идентификация и механизмы подтверждения подлинности пользователя; взаимная проверка подлинности пользователей; протоколы идентификации с нулевой передачей знаний.
17. Классификация и анализ проблем мобильных вычислительных систем.
18. Понятие «информационного оружия». Модели и методы проведения PsyOps.
19. Упрощенная схема идентификации с нулевой передачей знаний; проблема аутентификации данных и электронная цифровая подпись; однонаправленные хэш-функции; алгоритм безопасного деширования SHA;
20. Системы электронного документооборота.
21. Доктрина информационной безопасности 2016 года
22. Защита компьютерных систем от удаленных атак через сеть Internet. Режим функционирования межсетевых экранов и их основные компоненты;

маршрутизаторы; шлюзы сетевого уровня; усиленная аутентификация; основные схемы сетевой защиты на базе межсетевых экранов; применение межсетевых экранов для организации виртуальных корпоративных сетей; программные методы защиты.

23. Социальные сети и проблемы защиты информации в них.
24. Основные цели и задачи информационно-психологической войны.
25. Методы защиты программ от изучения и разрушающих программных воздействий (программных закладок и вирусов). Классификация способов защиты; защита от отладок и дизассемблирования; способы встраивания защитных механизмов в программное обеспечение;
26. Информационные войны. Противодействие информационному нападению.
27. Асимметричные системы шифрования.
28. Компьютерные вирусы как особый класс разрушающих программных воздействий; защита от РПВ; понятие изолированной программной среды.
29. Стратегические задачи науки, образования и культуры на этапе формирования информационного общества.
30. Глобализация общества и ее последствия.

РЕКОМЕНДУЕМЫЕ ИСТОЧНИКИ ИНФОРМАЦИИ

1. Хорев А.А. Техническая защита информации: учеб. пособие для студентов вузов. В 3 т. Том 1. Технические каналы утечки информации. - М.: НПЦ «Аналитика», 2008. - 436 с.: ил.
2. Шелухин, О.И. Обнаружение вторжений в компьютерные сети (сетевые аномалии) : учеб. пособие / Д.Ж. Сакалема, А.С. Филинова; О.И. Шелухин .— Москва : Горячая линия – Телеком, 2013 .— 221 с. : ил.
3. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации: Руководящий документ Гостехкомиссии России. М.: ГТК РФ, 1992.
4. ГОСТ Р 34.12-2015. Криптографическая защита информации. Блочные шифры.
5. ГОСТ Р 34.13-2015. Режимы работы блочных шифров.
6. ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.
7. ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хэширования.
8. Бабенко Л.К., Ищукова Е.А. Криптографическая защита информации: симметричное шифрование: учебное пособие // Таганрог: Изд-во ЮФУ, 2015. – 219 с.

9. Бабенко Л.К., Ищукова Е.А. Криптографические методы и средства обеспечения информационной безопасности, 2011. – Электронный ресурс, ссылка http://ntb.tgn.sfedu.ru/UML/UML_4789.pdf

10. Бабенко Л.К., Маро Е.А. Методы защиты приложений от несанкционированного использования с помощью аппаратных ключей HASP HL. Учебное пособие. Изд-во ЮФУ, 2015. 87 стр. Электронный ресурс, ссылка http://hub.sfedu.ru/allocator/files/d652ba29-ba89-4179-b82a-0a8a317a331f/predisplay/

11. Эриксон Д. Хакинг: искусство эксплоита. Пер. с англ. // СПб.: Символ-Плюс. 2005.

12. Золотарев В.В., Федорова Н.А. Анализ защищенности автоматизированных систем: Учебное пособие // СибГАУ. – Красноярск, 2007.

13. Макаревич О.Б. Гуманитарные аспекты информационной безопасности. Конспект лекций для аспирантов. ЮФУ г. Таганрог. Издательство ЮФУ,2017. – 88 с.

14. Стахнов А. А. Linux // 3-е изд., перераб. и доп. — СПб.: БХВ-Петербург, 2009.

15. Мандиа К., Просис К. Защита от вторжений. Расследование компьютерных преступлений // Изд. "Лори", 2005.

16. Нежданов, Игорь. Технологии информационных войн в Интернете // – Электронный ресурс, ссылка http://bash.rosmu.ru/activity/attach/events/1283/01.pdf.

17. Скиба В. Ю. Курбатов В. А. Руководство по защите от внутренних угроз информационной безопасности. // СПб.: Питер, 2008.

18. .Фостер Дж., Прайс М. Защита от взлома: сокеты, эксплойты, shell-код: Б. Шнайер, Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Издательство триумф, 2002 – 816 с.

19. Девянин П. Н. Модели безопасности компьютерных систем : управление доступом и информационными потоками : учеб. пособие для студ. вузов. - 2-е изд., испр. и доп.. - М. : Горячая Линия-Телеком, 2013. - 337 с. : ил.. - Библиогр.: с. 330-333 (48 назв.). - ISBN 978-5-9912-0328-9.

20. Фостер Дж., Лю В. Разработка средств безопасности и эксплойтов / Пер. с англ. // М.: Издательство «Русская Редакция» ; СПб. : Питер, 2007.