Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования
«Московский государственный технический университет имени Н.Э. Баумана»
(МГТУ им. Н.Э. Баумана)

УТВЕЖДАЮ
Первый проректор –
проректор по учебной работе
МГТУ им. Н.Э. Баумана

_____ Б.В. Падалкин

«_____» _____ 2015 г.

ПРОГРАММА ВСТУПИТЕЛЬНЫХ ИСПЫТАНИЙ В МАГИСТРАТУРУ

по направлению подготовки

10.04.01 Информационная безопасность

код и наименование направления подготовки

Факультет

Информатика и системы управления (ИУ)

Полное наименование факультета (сокращенное наименование)

Кафедра

Информационная безопасность (ИУ8)

Полное наименование кафедры (сокращенное наименование)

Москва, 2015 г.

1. ОБЩИЕ ПОЛОЖЕНИЯ

К вступительным испытаниям в магистратуру допускаются лица, имеющие документ государственного образца о высшем образовании любого уровня (диплом бакалавра или специалиста).

Лица, предъявившие диплом магистра, могут быть зачислены только на договорной основе.

Прием осуществляется на конкурсной основе по результатам вступительных испытаний.

Программа вступительных испытаний в магистратуру по направлению подготовки:

10.04.01 Информационная безопасность

код и наименование направления подготовки

составлена на основании Федерального государственного образовательного стандарта высшего образования подготовки бакалавра по направлению:

10.03.01 Информационная безопасность

код и наименование направления подготовки

и охватывает базовые дисциплины подготовки бакалавров по названному направлению.

Программа содержит описание формы вступительных испытаний, перечень вопросов для вступительных испытаний и список литературы рекомендуемой для подготовки.

2. ЦЕЛЬ ВСТУПИТЕЛЬНЫХ ИСПЫТАНИЙ

Вступительные испытания призваны определить степень готовности поступающего к освоению основной образовательной программы магистратуры по направлению:

10.04.01 Информационная безопасность

код и наименование направления подготовки

3. ФОРМА ПРОВЕДЕНИЯ ВСТУПИТЕЛЬНЫХ ИСПЫТАНИЙ

Вступительные испытания проводятся в письменной форме в соответствии с установленным приемной комиссией МГТУ расписанием.

Поступающему предлагается ответить письменно на 10 вопросов и задач билета, расположенных в порядке возрастания трудности и охватывающих содержание разделов и тем программы соответствующих вступительных испытаний.

На ответы по вопросам и задачам билета отводится **210 минут.**

Результаты испытаний оцениваются по **стобалльной** шкале.

Результаты испытаний оглашаются не позднее чем через три рабочих дня.

4. ПРОГРАММА ВСТУПИТЕЛЬНЫХ ИСПЫТАНИЙ

Письменное испытание проводится по программе, базирующейся на основной образовательной программе бакалавриата по направлению

10.03.01 Информационная безопасность

код и наименование направления подготовки

Перечень разделов и тем дисциплины, включенные в письменное испытание

ДИСЦИПЛИНА 1. Основы информационной безопасности

Система требований к информационной безопасности РФ и развитых стран мира

Введение. Современное состояние проблемы обеспечения информационной безопасности в автоматических системах. Информационное противоборство и правонарушения в области высоких технологий. Обеспечение доступности, конфиденциальности и целостности информации при передаче данных в каналах связи. Защита информации в операционных системах и компьютерных сетях. Нормативная база Российской Федерации по обеспечению информационной безопасности и защите информации. Грифы секретности. Классы защищенности автоматизированных систем и средств вычислительной техники. Контроль защищенности информационных ресурсов. Организационно-правовые меры по обеспечению информационной безопасности в РФ. Техническая защита информации. Криптографическая защита информации. Аудит информационной безопасности. Проблемы защиты персональных данных. Система требований к обеспечению защиты конфиденциальных сведений. Обеспечение информационной безопасности в США, «Оранжевая книга». Обобщенные критерии безопасных информационных технологий европейских стран. Обеспечение информационной безопасности других развитых стран мира. Проблема международной гармонизации стандартов в области обеспечения информационной безопасности.

Теоретические основы обеспечения информационной безопасности автоматизированных систем

Дискреционный и мандатный принципы доступа к информационным ресурсам. Принципы аутентификации в автоматизированных системах и подходы к разработке подсистем управления доступом. Модели управления доступом в автоматизированной системе: модель Белла – Ла Падулы, модель Харриссона - Руззо – Ульмана. Модели обеспечения целостности. Политика информационной безопасности организации, минимизация информационных рисков и модели противодействия злоумышленнику. Объекты и субъекты защиты информации. Разработка профилей защиты и заданий по безопасности для операционных систем, межсетевых экранов, средств доверенной загрузки. Задания по безопасности и их связь с профилями защиты. Классы и уровни безопасности при создании профилей защиты в соответствии с обобщенными критериями стандартами информационной безопасности России.

Программно-аппаратные средства обеспечения информационной безопасности автоматизированных систем

Программно-аппаратные средства обеспечения информационной безопасности. Системы обнаружения и предотвращения вторжений. Системы типа Snort. Системы с автоматическим ответом. Принципы информационной фильтрации и межсетевое экранирование. Принципы построения антивирусных средств. Интеграция средств защиты, создание ядра безопасности. Маскирование информации и стеганография. Защита персональных данных и конфиденциальной информации с помощью средств защиты от нарушений целостности. Кодирование информации при передаче по линиям связи. Серверы безопасности и

автоматизированные рабочие места администратора информационной безопасности. Дефекты и некорректности в программном обеспечении. Классификация технических каналов утечки информации задачи противодействия техническим разведкам. Побочные электромагнитные излучения и наводки. Соотношение «сигнал – шум» и выделение полезного сигнала из спектра. Утечка акустической информации и противодействие ей: звукоизоляция и звукопоглощение. Принципы зашумления сигнала и защита помещения. Поиск аппаратурных закладок в помещениях и в аппаратуре. Утечки видовой информации и противодействие им. Принципы организации защищенных периметров. Категорирование служебных и производственных помещений. Задачи охранной сигнализации и принципы ее разработки и функционирования.

Перечень вопросов.

1. Виды, источники и носители защищаемой информации.
2. Обеспечение доступности, конфиденциальности и целостности информации при передаче данных в каналах связи.
3. Защита информации в операционных системах и компьютерных сетях.
4. Грифы секретности.
5. Классы защищенности автоматизированных систем и средств вычислительной техники.
6. Организационно-правовые меры по обеспечению информационной безопасности в РФ.
7. Техническая защита информации.
8. Криптографическая защита информации.
9. Аудит информационной безопасности.
10. Проблемы защиты персональных данных.
11. Система требований к обеспечению защиты конфиденциальных сведений.
12. Обеспечение информационной безопасности в США, «Оранжевая книга».
13. Обобщенные критерии безопасных информационных технологий европейских стран.
14. Дискреционный и мандатный принципы доступа к информационным ресурсам.
15. Принципы аутентификации в автоматизированных системах и подходы к разработке подсистем управления доступом.
16. Модели управления доступом в автоматизированной системе: модель Белла – Ла Падулы, модель Харриссона - Руззо – Ульмана.
17. Модели обеспечения целостности.
18. Политика информационной безопасности организации, минимизация информационных рисков и модели противодействия злоумышленнику.
19. Объекты и субъекты защиты информации.
20. Разработка профилей защиты и заданий по безопасности для операционных систем, межсетевых экранов, средств доверенной загрузки.
21. Задания по безопасности и их связь с профилями защиты.
22. Классы и уровни безопасности при создании профилей защиты в соответствии с обобщенными критериями стандартами информационной безопасности России.
23. Программно-аппаратные средства обеспечения информационной безопасности.
24. Системы обнаружения и предотвращения вторжений.
25. Системы типа Snort.
26. Принципы информационной фильтрации и межсетевое экранирование.
27. Принципы построения антивирусных средств.
28. Интеграция средств защиты, создание ядра безопасности.

29. Маскирование информации и стеганография.
30. Защита персональных данных и конфиденциальной информации с помощью средств защиты от нарушений целостности.
31. Помехоустойчивое кодирование информации при передаче по линиям связи.
32. Серверы безопасности и автоматизированные рабочие места администратора информационной безопасности.
33. Дефекты и некорректности в программном обеспечении.
34. Классификация технических каналов утечки информации, задачи противодействия техническим разведкам.
35. Побочные электромагнитные излучения и наводки.
36. Соотношение «сигнал – шум» и выделение полезного сигнала из спектра.
37. Утечка акустической информации и противодействие ей: звукоизоляция и звукопоглощение.
38. Принципы зашумления сигнала и защита помещения.
39. Поиск аппаратурных закладок в помещениях и в аппаратуре.
40. Утечки видовой информации и противодействие им.
41. Принципы организации защищенных периметров. Категорирование служебных и производственных помещений.
42. Задачи охранной сигнализации и принципы ее разработки и функционирования.
43. Демаскирующие признаки объектов защиты информации.

Основная учебная литература.

1. Ховард М., Лебланк Д.. Защищённый код. – Москва: «Русская редакция». – 2011.
2. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа - Санкт-Петербург: «Наука и Техника». - 2011

Дополнительная учебная литература.

1. Padula Len La. Secure Computer Systems: A Mathematical Model. - USA. - 1996
2. Rehman Rafeeq Ur. Intrusion Detection Systems with Snort - USA: «Open Source». - 2010
3. Security Engineering: A Guide to Building Dependable Distributed Systems
4. Tulloch M. Microsoft Encyclopedia of Security - USA: «Microsoft Pres». - 2010
5. Wesley W. Managing Information Security Risks: The OCTAVE Approach - USA: «The Software Engineering Institute». - 2002
6. Грушо А., Тимонина Е. Теоретические основы защиты информации - Москва: «Яхтсмен». - 2005

Автор(ы) программы:

Булдакова Т.И д.т.н., профессор
Басараб М.А. д. ф.-м.н., доцент
Быков А.Ю. к.т.н., доцент

Декан факультета		А.В. Пролетарский
Заведующий кафедрой		В.А. Матвеев
Начальник отдела магистратуры		Б.П. Назаренко