МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

ФГБОУ ВПО «Брянский государственный технический университет»

УТВЕРЖДАЮ
Ректор университета
О.Н. Федонин
от «31» 03 2016 г.

ПРОГРАММА
вступительного испытания в аспирантуру

по направлению подготовки кадров высшей квалификации – программы подготовки научно-педагогических кадров в аспирантуре

10.06.01 «Информационная безопасность»,

профиль подготовки «Методы и системы защиты информации, информационная безопасность»

Технические науки

Брянск 2016

Программа вступительного испытания по профилю подготовки «Методы и системы защиты информации, информационная безопасность» - Брянск: БГТУ, 2016.- 9 с.

Программу разработал
к.т.н., доцент _____/М.Ю. Рытов/

Программа утверждена на заседании кафедры «Системы информационной безопасности» ФГБОУ ВПО БГТУ (протокол № 8 от «23» марта 2016).

Заведующий кафедрой «СИБ»
к.т.н., доцент _____/М.Ю. Рытов/

СОГЛАСОВАНО:
Проректор по научной работе,
к.т.н., доцент _____/В.М. Сканцев/

Программа вступительного экзамена по профилю подготовки «Методы и системы защиты информации, информационная безопасность» составлена согласно паспорту научной специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность». В программе учитываются указанные в паспорте области исследования.

Программа отражает современное состояние обеспечения информационной безопасности и включает важнейшие общенаучные разделы, знание которых необходимо специалисту в этой области. Рассмотрение проблем защиты информации и информационной безопасности базируется на задачах ускорения научно-технического прогресса и в частности – на необходимости решения данных проблем в связи с интенсивной информатизацией современного общества и происходящими изменениями в стране.

Цель программы вступительного испытания:

Установить объем и уровень знаний экзаменуемого поступающего в аспирантуру по специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность» для оценки его способностей к самостоятельному исследованию в области информационной безопасности.

Задачи программы вступительного испытания

- сформулировать требования к знаниям, умениям и навыкам экзаменуемого в области информационной безопасности;
- определить состав тем, охват которых обеспечивает требуемую компетенцию соискателя;
- определить содержание каждой темы;
- привести список литературы, достаточный для освоения тем в нужном объеме.

Требования к уровню знаний экзаменуемого:

Экзаменуемый должен знать:

- основные информационные технологии используемые в автоматизированных системах;
- языки программирования высокого уровня (объектно-ориентированное программирование);
- основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в компьютерных сетях;
- средства обеспечения безопасности данных;
- источники и классификацию угроз информационной безопасности;
- основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации;

- основные задачи и понятия криптографии;
- требования к шифрам и основные характеристики шифров;
- технические каналы утечки информации;
- возможности технических средств перехвата информации;
- организацию защиты информации от утечки по техническим каналам на объектах информатизации;
- основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации;
- программно-аппаратные средства обеспечения информационной безопасности;
- основные угрозы безопасности информации и модели нарушителя в автоматизированных системах.

Уметь:

- оценивать эффективность и надежность средств защиты;
- классифицировать и оценивать угрозы информационной безопасности для объекта информатизации;
- эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах;
- применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности;
- проводить выбор программно-аппаратных средств обеспечения информационной безопасности для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы;
- разрабатывать и исследовать аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем;
- исследовать эффективность создаваемых систем информационной безопасности автоматизированных систем и проводить технико-экономическое обоснование проектных решений;
- разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем;
- разрабатывать модели угроз и нарушителей информационной безопасности автоматизированных систем;
- выявлять уязвимости информационно-технологических ресурсов автоматизированных систем, проводить мониторинг угроз безопасности автоматизированных систем.

Владеть:

- профессиональной терминологией в области информационной безопасности;
- навыками работы с нормативно-правовыми актами;
- навыками организации и обеспечения режима секретности;
- методами организации и управления деятельностью служб защиты информации на предприятии;
- методами формирования требований по защите информации;
- методами и технологиями проектирования, моделирования, исследования автоматизированных систем и подсистем безопасности автоматизированных систем;
- навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем;
- методами мониторинга и аудита выявления угроз информационной безопасности автоматизированных систем;
- методами управления информационной безопасностью автоматизированных систем;
- методами оценки информационных рисков;
- навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем.

Форма проведения

Испытание осуществляется в форме экзамена - письменного изложения ответов на содержащиеся в настоящей программе вопросы и собеседования (4 вопроса).

Продолжительность экзамена - 1 час.

При подготовке ответа экзаменующемуся разрешается пользоваться справочниками, ГОСТами и другой нормативно-технической литературой.

Содержание вступительного испытания

В основу настоящей программы положены следующие дисциплины: «Системы обнаружения вторжений»; «Комплексное обеспечение информационной безопасности автоматизированных систем»; «Криптографические методы защиты информации», «Организационное обеспечение информационной безопасности», «Безопасность систем баз данных», «Безопасность операционных систем», «Программно-аппаратные средства обеспечения информационной безопасности», «Технические средства и методы защиты информации».

Раздел 1 «Избранные разделы математики и информатики»

Информация, сообщения, информационные системы и процессы как объекты информационной безопасности. Основные свойства информации.

Мера количества информации. Энтропия. Случайные события. Полная группа событий. Зависимые и независимые случайные события. Вероятность случайного события. Условная вероятность. Формула полной вероятности. Теорема Байеса. Случайные величины и их характеристики: функция распределения, моменты, характеристические функции. Дискретные и непрерывные случайные величины. Биноминальный закон распределения. Нормальный закон распределения. Центральная предельная теорема Ляпунова. Основные задачи математической статистики: точечная оценка, построение доверительного интервала, различение статистических гипотез. Сетевая модель OSI/ISO. Уровни модели OSI.Сетевая модель OSI/ISO. Примеры протоколов.

Раздел 2 «Теоретические основы информационной безопасности»

Понятие угрозы информационной безопасности. Виды угроз. Основные методы реализации угроз информационной безопасности. Основные принципы обеспечения информационной безопасности в АС. Методы оценки угроз ИБ. Модель угроз. Причины, виды и каналы утечки информации. Построение систем защиты от угрозы нарушения конфиденциальности информации. Обобщенная модель нарушителя. Методы оценки риска. Методы обнаружения, локализации и ликвидации угроз информационной безопасности. Общие требования по обеспечению информационной безопасности. Профиль защиты и задание по обеспечению безопасности, их структура и взаимосвязи между ними. Политика и задачи безопасности, их взаимосвязь. Функциональные и гарантийные требования безопасности. Анализ безопасности программ. Методы анализа безопасности программного обеспечения. Логико-аналитические методы анализа безопасности программного обеспечения. Модели разграничения доступа. Методы контроля доступа. Модели контроля целостности. Модель Биба. Модель Кларка-Вилсона.Построение систем защиты от угрозы нарушения целостности информации. Построение систем защиты от угрозы отказа доступа к информации. Политика безопасности. Понятие политики безопасности. Понятия доступа и монитора безопасности. Основные типы политики безопасности. Модели безопасности. Модель матрицы доступов HRU. Модель распространения прав доступа Take-Grant. Модель системы безопасности Белла-Лападула. Основные критерии защищенности АС. Классификация систем защиты АС. Руководящие документы Государственной технической комиссии России. Общие критерии (ОК). Основные положении ОК.

Раздел 3 «Основы криптографической защиты информации»

Криптографические методы зашиты информации. Основные понятия криптографии. Исторические шифры. Теоретическая, практическая и вре-

менная стойкость системы криптографической защиты. Методы получения псевдослучайных последовательностей. Современные поточные и блочные алгоритмы шифрования. Системы симметричного шифрования. Системы асимметричного шифрования, открытый ключ, электронная подпись. Вопросы генерации и распределения ключей. Обоснование надежности криптографической защиты.

Примерные вопросы для вступительного экзамена

1. Структура государственных органов, обеспечивающих безопасность информационных технологий.
2. Этапы создания комплексной системы защиты информации.
3. Организация работ с конфиденциальными информационными ресурсами на объектах информатизации.
4. Защита от злоумышленных действий обслуживающего персонала и пользователей.
5. Выбор показателей эффективности и критериев оптимальности КСЗИ.
6. Понятие криптосистемы. Классификация криптосистем. Основные требования к шифрам.
7. Основные алгебраические структуры, используемые в криптографии. Группы, кольца, конечные поля. Конечные группы точек эллиптической кривой.
8. Поточные шифры, табличное и модульное гаммирование. Случайные и псевдослучайные гаммы.
9. Криптографические стандарты. (Блочный алгоритм шифрования, криптографическая хэш-функция, алгоритмы цифровой подписи на основе мультипликативной группы конечного поля и группы точек эллиптической кривой).
10. Генераторы случайных и псевдослучайных последовательностей.
11. Криптографические хэш-функции.
12. Общая характеристика организационных методов защиты информации.
13. Классификация угроз информационной безопасности. Виды КУИ.
14. Требования к построению систем безопасности предприятия. Цели и задачи системы безопасности объекта. Виды объектов защиты.
15. Характеристика типовой структуры службы безопасности. Основные задачи службы безопасности объекта. Характеристика функций службы безопасности объекта.

16. Организация режима и охраны на объекте. Основные задачи. Виды пропускных документов. Порядок организации пропускного режима.

17. Аттестация объектов информатизации.

18. Характеристика информационно-аналитической работы. Основные направления аналитической работы на объекте защиты.

19. Виды персональных данных в соответствии с ФЗ № 152 «О персональных данных». Основные этапы создания СЗПДн на объекте информатизации.

20. Виды и характеристика конфиденциальной информации в РФ.

21. Свойства информации, как объекта защиты. Характеристика основных источников информации.

22. Классификация и характеристика технических каналов утечки информации

23. Основные методы защиты информации техническими средствами.

24. Способы и средства противодействия наблюдению.

25. Способы и средства противодействия подслушиванию.

26. Способы и средства предотвращения записи речи на диктофон и через закладные устройства.

27. Виды закладных устройств. Основные признаки закладных устройств. Средства борьбы с радиозакладками. Способы их подавления. Способы контроля помещений на отсутствие закладных устройств.

28. Технические средства обеспечения охраны объектов.

29. Способы и средства инженерной защиты объектов.

30. Классификация и основные элементы телевизионных систем наблюдения.

Учебно-методическое и информационное обеспечение программы

Основная литература

1. Аверченков В.И., Автоматизация проектирования комплексных систем защиты информации: монография / В.И. Аверченков, М.Ю. Рытов, О.М. Голоембиовская. – Брянск: БГТУ, 2012 – 143 с.

2. Гулак, М.Л. Основы компьютерной безопасности: учебное пособие / М.Л. Гулак, М.Ю. Рытов. – Брянск: БГТУ, 2013. – 216 с.

3. Аверченков В.И. Аудит информационной безопасности: учеб. Пособие / В.И. Аверченков. – Брянск: БГТУ, 2010 – 269 с.

4. Аверченков В.И. Организационная защита информации: учеб. Пособие / В.И. Аверченков, М.Ю. Рытов – Брянск: БГТУ, 2010 – 184с.

5. Аверченков В.И., Служба защиты информации: организация и управление: учеб. пособие / В.И. Аверченков, М.Ю. Рытов. – Брянск: БГТУ, 2010 – 186с.

Дополнительная литература

1. Аверченков В.И. Системы защиты информации в ведущих зарубежных странах: учеб.пособие для вузов / В.И. Аверченков, М.Ю. Рытов, Г.В. Кондрашин, М.В. Рудановский. – Брянск: БГТУ, 2010 – 225 с.

2. Аверченков В.И. Разработка системы технической защиты информации/ В.И. Аверченков, М.Ю. Рытов, А.В. Кувыклин, Т.Р. Гайнулин. – Брянск: БГТУ, 2009. – 187 с. – (Серия «Организация и технология защиты информации»).

3. Аверченков В.И. Методы и средства инженерно-технической защиты информации / В.И. Аверченков, М.Ю. Рытов, А.В. Кувыклин, Т.Р. Гайнулин. – Брянск: БГТУ, 2009. – 187 с. – (Серия «Организация и технология защиты информации»).

4. Аверченков В.И. Защита персональных данных в организации: монография/ В.И. Аверченков, М.Ю. Рытов, Т.Р. Гайнулин. – Брянск: БГТУ, 2010. – 124 с.– (Серия «Организация и технология защиты информации»).

5. Аверченков В.И. Аудит информационной безопасности органов системы государственного и муниципального управления: монография / В.И. Аверченков, М.Ю. Рытов, Г.В. Кондрашин, М.В. Рудановский. – Брянск: БГТУ, 2009. –126 с.

Интернет-ресурсы

1. www.fstek.ru – официальный сайт ФСТЭК России.

2. www.egovernment.ru - Интернет-журнал «Информационная безопасность».

3. www.law.yarovoiy.com - - Интернет - сайт “Все законы России”.

4. www.rg.ru – Интернет-сайт «Российской газеты».