Федеральное государственное автономное образовательное учреждение высшего образования
Национальный исследовательский университет
«Высшая школа экономики»

Утверждаю
Проректор НИУ ВШЭ
С.Ю. Рощин

_____

Одобрено на заседании
академического совета
аспирантской школы
по техническим наукам
протокол № 03/2 от 29.03.2016

Согласовано
Академический директор
Аспирантской школы
по техническим наукам
Клышинский Э.С.

_____

Программа
вступительного испытания по специальной дисциплине для поступающих на обучение по программам подготовки научно-педагогических кадров в аспирантуре

Направление - 10.06.01 – Информационная безопасность,
Профиль (направленность) - 05.13.19 Методы и системы защиты информации, информационная безопасность

Москва
2016

1. Область применения и нормативные ссылки

Настоящая программа разработана в соответствии с Программой-минимум кандидатского экзамена по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность» и Паспорта научной специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

2. Структура вступительного экзамена

Форма проведения экзамена: устный

Структура вступительного экзамена:

Экзамен состоит из ответа на билет, содержащий из три вопроса. Экзаменуемый отвечает на вопросы, указанные в билете, и отвечает на вопросы комиссии.

Оценка уровня знаний (баллы):

Каждый вопрос оценивается по десятибалльной шкале. Итоговая оценка выставляется по 5-бальной шкале по следующему принципу пересчета:

"Отлично" - 8-10 баллов (по 10-балльной шкале);

"Хорошо" - 6-7 баллов (по 10-балльной шкале);

"Удовлетворительно" - 4-5 баллов (по 10-балльной шкале);

"Неудовлетворительно" - 0-3 балла (по 10-балльной шкале).

Критерии оценивания

	Баллы
Ответ полный без замечаний, продемонстрированы знания ….	10-8
Ответ полный, с незначительными замечаниями,…	6-7
Ответ не полный, существенные замечания,…	4-5
Ответ на поставленный вопрос не дан.	0-3

Невыполнение одного из заданий (или отказ от его выполнения) является, как правило, основанием для выставления неудовлетворительной оценки за кандидатский экзамен в целом.

3. Содержание

1.Теоретические основы защиты информации

1. *Основные принципы современной концепции обеспечения защиты информации*. Исходные предположения о возможностях злоумышленника. Требования к защите с позиции пользователя. Основные методы защиты.
2. *Роль законодательного и организационного обеспечения защиты информации*. Законы Российской Федерации, составляющие основу правовой базы защиты информации в стране. Особенности российского законодательства в части защиты государственной тайны, коммерческой тайны и авторских прав. Порядок лицензирования и сертификации деятельности в области защиты информации.
3. *Математические модели формальной теории защиты информации*. Угрозы информации и политика безопасности. Классификация систем защиты. Стандарты в области защиты информации в вычислительной системе, «Оранжевая книга» США, российские стандарты.
4. *Криптографические методы защиты информации*. Основные понятия криптографии. Исторические шифры. Теоретическая, практическая и временная стойкость системы криптографической защиты. Методы получения псевдослучайных последовательностей. Современные поточные и блочные алгоритмы шифрования. Системы ассиметричного шифрования, открытый ключ, электронная подпись. Вопросы генерации и распределения ключей. Атаки на криптографические алгоритмы: алгоритмические, алгебраические, статистические. Методология обоснования надежность криптографической защиты.
5. *Криптографические протоколы.* Криптографические протоколы с использованием симметричного и асимметричного шифрования. Криптографические протоколы с использованием цифровой подписи. Криптографические протоколы генерации и распределения ключей. Протоколы разделения секрета и доказательства без разглашения.
6. *Программно-аппаратные средства обеспечения информационной безопасности*. Методы и средства ограничения доступа к компонентам ЭВМ. Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям. Методы и средства хранения ключевой информации. Средства обеспечения безопасности в ОС семейств Windows и UNIX, критерии защищенности ОС. Средства обеспечения безопасности в сетях. Протоколы аутентификации при удаленном доступе. Средства защиты серверов и рабочих станций. Средства защиты локальных сетей при подключении к Internet. Межсетевые экраны, электронные замки, криптофильтры, криптороутеры. Области применения, достоинства, недостатки, реализуемые политики безопасности. Методы оценки качества применяемых средств защиты. Методы и средства защиты информации в СУБД. Средства идентификации и аутентификации, управление доступом, средства контроля, аудит безопасности. Критерии защищенности БД и АИС.
7. *Защита информации от технической разведки*. Основные физические каналы утечки информации о функционировании информационной системы. Узлы и блоки оборудования информационной системы, уязвимые для технической разведки. Технические параметры современных средств перехвата побочных сигналов. Методы и средства защиты от инженерно-технической разведки. Методика оценки качества инженерно-технической защиты.
8. *Особенности защиты информации в вычислительной системе*. Перечень типовых угроз вычислительной системе со стороны потенциального злоумышленника. Основные принципы защиты вычислительной системы от несанкционированного доступа (проверка полномочий, разграничение доступа, аудит). Защита информации в локальных и глобальных вычислительных сетях и ее особенности. Роль и задачи администратора вычислительной системы и службы безопасности.
9. *Разрушающие программные воздействия.* Компьютерные вирусы как особый класс разрушающих программных воздействий. Классификация вирусов. Методы выявления и защиты от вирусов. Изолированные программные среды. Защита программных продуктов от изменения и контроль целостности, защита от изучения.

2. Теория вероятностей и математическая статистика

1. Вероятность: аксиомы и свойства (дискретный, абсолютно-непрерывный и общий случаи).
2. Случайные величины и их характеристики: определение, свойства (дискретный, абсолютно-непрерывный и общий случаи, функции распределения, моменты).
3. Основные вероятностные распределения, их свойства (нормальное, биномиальное, экспоненциальное, пуассоновское, связь между ними)
4. Предельные теоремы: закон больших чисел, теоремы Хинчина, Чебышева; усиленный закон больших чисел, теорема Колмогорова; центральная предельная теорема, теорема Муавра-Лапласа.
5. Характеристические функции, их свойства, связь с моментами.
6. Выборка, эмпирическая функция распределения, гистограмма.
7. Критерии отношения правдоподобия, его основные асимптотические свойства, его связь с критерием хи-квадрат для полиномиального распределения.
8. Лемма Неймана-Пирсона; равномерно наиболее мощные (р.н.м.) критерии для моделей с монотонным отношением правдоподобия в случае односторонних гипотез; двусторонние гипотезы, несмещенные критерии для них.
9. Критерии согласия Колмогорова, хи-квадрат, Смирнова и др. для гипотез о виде распределения, односторонности, независимости, случайности.
10. Доверительные интервалы и множества, построение доверительных интервалов с помощью центральной статистики, примеры; асимптотические доверительные интервалы.
11. Случайные подстановки, методы генерации. Циклы в случайных подстановках, распределение числа циклов.
12. Применение вероятностных методов в теории защиты информации: построение вероятностных моделей процессов, возникающих в задачах защиты информации, проверка качества псевдослучайных последовательностей и др.

3. Алгебра.

1. Группа, подгруппа, нормальный делитель, фактор-группа. Циклическая группа; абелева группа (определения, примеры), гомоморфизм групп. Группа подстановок.
2. Идеал кольца, гомоморфизм колец, кольцо многочленов, разложение на множители, интерполяционная формула Лагранжа. Разложение кольца вычетов по заданному модулю в прямую сумму колец.
3. Простое поле, расширение поля, примитивный элемент конечного поля, описание множества примитивных элементов через степени одного из них. Алгоритмы построения примитивных элементов. «Китайская» теорема об остатках, методы разложения многочленов на неприводимые множители.
4. Линейные рекуррентные последовательности над конечным полем. Характеристический и минимальный многочлен, сопровождающая матрица. Оценка длины периода.
5. Применение алгебраических методов в задачах защиты информации.

4. Теория информации.

1. Энтропия вероятностной схемы. Условная энтропия. Взаимная, собственная, условная информация вероятностных схем.
2. Математические модели дискретных источников сообщений. Эргодические источники. Теорема Шеннона для источников без памяти.
3. Классификация каналов связи. Пропускная способность. Пропускная способность дискретного канала без памяти.

Литература и источники

1. Кабанов А.С., Лось А.Б., Першаков А.С., Теоретические основы компьютерной безопасности, М: РИО МИЭМ, 2012 г.
2. Девянин П.Н., Ивашко А.М., Першаков А.С., Проскурин В.Г., Черемушкин А.В.

Программно-аппаратные средства защиты от НСД к компьютерным криптографическим системам обработки информации (учебное пособие), МИЭМ, 2003.
3. Проскурин В.Г., Защита программ и данных, ИД «Академия», 2011 г.
4. Алфёров А.П., Зубов А.Ю., Кузьмин А.С., Черёмушкин А.В. Основы криптографии. М.: Гелиос АРВ, 2005.
5. Духин А.А. Теория информации (учебное пособие), МИЭМ, 2005 г.
6. Зубов А.Ю. Математики кодов аутентификации, М. :Гелиос АРВ, 2007.
7. Законы РФ «О государственной тайне», «Об информации, информационных технологиях и защите информации», «О стандартизации». Положения о лицензировании ФСБ и ФСТЭК.
8. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем, М: горячая линия – Телеком, 2000 г.
9.Фомичев В.М. Дискретная математика и криптология. М.: "ДИАЛОГ· МИФИ", 2003.
10. Девянин П.Н. Модели безопасности компьютерных систем, М.: Издательский центр «Академия», 2005.
11. Корт С.С. Теоретические основы защиты информации: Учебное пособие, М.: Гелиос АРВ, 2004.
12. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие, М.: ИД «ФОРУМ»: ИНФРА-М, 2008.
13. W. Stallings Cryptography and Network Security, Prentice Hall, Upper Saddle River, New Jersey 07458, 2001, 669 p.
14. B. Scheier Applied cryptography, John Wiley&Sons, Inc, 2002, 815 p.
15. Boycott Starforce. http://www.glop.org/starforce/.
16. Honeyd Vs MSBLAST.EXE. http://www.citi.umich.edu/u/provos/honeyd/msblast.html.
17. MSBlast epidemic far larger than believed. http://news.zdnet.com/2100-1009_22-5184439.html.