МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
РАДІОЕЛЕКТРОНІКИ

ЗАТВЕРДЖУЮ
Голова приймальної
комісії ХНУРЕ
_____Е.Ю. Рубін
«___» _____ 2016 р.

ПРОГРАМА
ВСТУПНОГО ІСПИТУ ДО АСПІРАНТУРИ

Спеціальність 125 – Кібербезпека_____

Протокол засідання приймальної комісії

№ ____ від _____ 20__ р.

Зав. відділом аспірантури
та докторантури _____В.П. Манаков
(підпис, ініціали, прізвище)

Відповідальний секретар
приймальної комісії _____А.В.Снігуров
(підпис, ініціали, прізвище)

Харків 2016

Програма розроблена авторським колективом у складі: Халімов Г.З. – доктор технічних наук (Харківський національний університет радіоелектроніки), Горбенко І.Д. – доктор технічних наук (Харківський національний університет радіоелектроніки), Олійников Р.В. – доктор технічних наук (Харківський національний університет радіоелектроніки), Поповський В.В. – доктор технічних наук (Харківський національний університет радіоелектроніки).

Програма затверджена Вченою радою Харківського національний університету радіоелектроніки “___”_____2016 р. Протокол № _____.

ПРОГРАМА

вступного іспиту до аспірантури за спеціальністю 125 – «Кібербезпека»

1. Спецрозділи математики

1.1. Основи теорії чисел

1.1.1. Поняття подільності чисел. Ділення із залишком. НСД двох чисел. Знаходження НСД двох чисел. Спільне найменше кратне.

1.1.2. Прості числа. Великі прості числа. Методи побудови «великих» простих чисел. Псевдопрості числа, головні методи їхньої побудови.

1.1.3. Функція Ейлера. Узагальнена функція Ейлера. Визначення та головні властивості.

1.2.Основи теорії груп, кілець та полів

1.2.1. Групи, головні поняття та визначення. Мультиплікативні групи. Підстановки. Групи підстановок. Підгрупи.

1.2.2. Кільця, визначення та властивості. Кільце з одиницею. Ізоморфні кільця.

1.2.3. Поля, визначення та властивості. Прості та поширені поля.

1.2.4. Еліптичні криві, визначення та властивості.

1.3.Теорія ймовірності та мат. статистики

1.3.1. Дискретно-ймовірнісний простір. Події та ймовірності, їх визначення та властивості. Приклади розподілів. Випадкові величини. Мат. очікування. Незалежні випадкові величини.

1.3.2. Основні поняття мат. статистики. Закони розподілу ймовірностей. Біноміальний, показовий, рівномірний та нормальний розподіл.

1.3.3. Перевірка статистичних гіпотез. Схема іспитів Бернуллі, критерій знаків для однієї вибірки. Критерій згоди Колмогорова, x^2 – квадрат Пірсона.

1.4. Спеціальний розділ теорії інформації

1.4.1. Умовна та безумовна ентропія. Умовна апостеріорна ентропія. Середня взаємна інформація.

1.4.2. Блокові та не блокові коди. Норми, метрики та кодові відстані. Лінійні коди, згорткові коди.

1.4.3. Псевдовипадкові послідовності. Лінійні та нелінійні рекурентні послідовності, їх властивості.

1.5. Алгоритмічні основи криптографії

1.5.1. Основні методи обчислень в багатослівній арифметиці та оцінка їх складності.

1.5.2. Методи побудування «великих» простих чисел та незвідних поліномів, складність та реалізація алгоритмів.

1.5.3. Афінний та проективний базиси скалярного множення в групі точок еліптичних кривих.

1.5.4. Методи побудування системних параметрів для криптографічних додатків на еліптичних кривих.

1.5.5. Методи розв’язку дискретних логарифмічних рівнянь в групі точок еліптичних кривих та порівняльна оцінка їх складності.

1.6. Теорія ймовірних процесів

1.6.1. Основні характеристики процесів. Представлення процесів в просторі станів. Егодичні процеси. Часові та частотні моделі процесів.

1.6.2. Марківські моделі процесів. Рівняння стану. Дискретні та безперевні представлення.

1.6.3. Методи обробки ймовірних процесів. Стохастична апроксимація. Рекуретне оцінювання. Фильтри Калмана-Б'юсі.

1.6.4. Методи оптимального управління динамічними системами. Критерії ефективності. Теорема про розділення.

1.6.5. Рівняння Ерланга. Системи масового обслуговування.

1.7. Теорія штучного інтелекту

1.7.1. Аналіз, синтез і моделювання нейронних мереж, розроблення методів їх проектування, оптимізації та навчання.

1.7.2. Експертні технології прийняття рішень

1.7.3. Представлення знань у вигляді правил (продукційна модель)

2. Методи та засоби захисту інформації. Криптографічні системи

2.1. Основи теорії захисту інформації

2.1.1 Моделі загроз та порушника. Фактори уразливості та канали витоку інформації, шляхи несанкціонованого доступу. Концепція захищеної комп'ютерної системи (мережі). Політики безпеки інформації та їх впровадження.

2.1.2 Основні функції криптографічних систем. Криптографія та криптографічний аналіз. Класифікація криптографічних систем по стійкості.

2.1.3 Теоретично не дешифруємі системи й умови їхньої реалізації.

2.1.4 Обчислювально-стійкі та доказово стійкі системи й умови їхньої реалізації.

2.1.5 Інформаційні характеристики джерел повідомлень, криптограм і ключів.

2.1.6 Класифікація шифрів. Симетричні та асиметричні шифри. Блокові та потокові шифри.

2.1.7 Потокові симетричні шифри та їхні властивості. Генератори псевдовипадкових послідовностей. Блокові симетричні шифри та їхні властивості.

2.1.8Асиметричні шифри та їхні властивості. Умови реалізації й галузі застосування систем шифрування з відкритими ключами та відкритим поширенням ключів.

2.1.9. Ідентифікація й автентифікація. Погрози порушення автентичності. Модель взаємної довіри, взаємної недовіри та взаємного захисту.

2.1.10. Симетричні системи автентифікації. Методи автентифікації в потокових системах шифрування, оцінка їхньої ефективності.

2.1.11. Цифровий підпис і його реалізація. Оцінка ефективності цифрових підписів.

2.1.12. Класифікація методів криптографічного аналізу та умови здійснення.

2.2. Криптографічні системи

2.2.1. Класифікація та характеристика симетричних криптографічних систем. Основні вимоги та склад симетричних криптографічних систем.

2.2.2. Основні принципи та режими симетричного шифрування.

2.2.3. Алгоритми та засоби формування ключових даних. Вимоги до ключових даних.

2.2.4. Класифікація та характеристика асиметричних криптографічних систем. Методи направленого шифрування.

2.2.5. Системи з відкритим поширенням ключів. Основні протоколи встановлення таємниці та ключів. Аналіз рівнів безпеки.

2.2.6. Алгоритми цифрового підпису в класі криптосистем Ель - Гамаля та порівняльний аналіз їх властивостей.

2.2.7. Алгоритм цифрового підпису в групі точок еліптичних кривих. Криптографічна стійкість та складність перетворень.

2.2.8. Класифікація, суть та порівняльний аналіз стандартних алгоритмів та засобів гешування.

2.3. Проектування та використання систем і засобів захисту інформації

2.3.1. Нормативна база, яка визначає процеси розробки та створення комплексних систем захисту інформації.

2.3.2. Вимоги до перспективних симетричних криптографічних систем. Стандарти симетричного блокового шифрування.

2.3.3. Стійкість симетричних блокових криптосистем. Методика оцінки та порівняльного аналізу.

2.3.4. Розробка програмних і апаратних засобів криптографічного захисту інформації. Основні вимоги. Принципи програмної та апаратної реалізації.

2.3.5. Інфраструктури відкритих ключів, призначення, вимоги та принципи функціонування.

2.3.6. Комплексні системи захисту центрів сертифікації ключів, вимоги до них, порядок створення і застосування

2.4. Технічний захист інформації.

2.4.1. Структура систем і аналіз можливих каналів витоку інформації. Безпека випромінювань та наводок.

2.4.2. Класифікація засобів ТЗІ. Критерії безпеки. Вплив екранів і заземлення на рівень випромінювання електромагнітних полів.

2.4.3 Організаційні засоби по технічному захисті інформації.

2.4.4 Вимоги та методи забезпечення захисту інформації від витоку по технічним каналам в АС 1та АС2.

2.4.5. Вимоги нормативних документів та захист електронних засобів інформаційно – телекомунікаційних систем від зовнішнього впливу.

2.5. Системи керування захистом інформації

2.5.1. Архітектура системи безпеки операційних систем (ОС).

2.5.2. Диспетчер облікових записів (ДОЗ). Паролі, відновлення паролів.

2.5.3. Захист файлів і компоненти (NTFS). Права доступу. Дозволи NTFS.

2.5.4. Захист реєстру. Інформація про безпеку реєстру. Захист від локального та віддаленого доступу. Аудит реєстру.

3. Захист інформації в системах і мережах

3.1. Стандартизація та сертифікація систем і засобів захисту інформації

3.1.1 Основні положення безпеки інформації. Сутність вимог основних стандартів по забезпеченню безпеки інформації.

3.1.2 Призначення та ціль розробки стандарту. Етапи розробки стандартів. Порядок сертифікації засобів захисту.

3.1.3 Основні вимоги стандартів по управлінню ключами. Функції центрів управління та сертифікації ключів.

3.1.4 Стандарти ЕЦП та їх застосування.

3.1.5 Стандартні криптографічні протоколи розподілу таємниці. Властивості та реалізація.

3.1.6 Стандарти гешування, властивості та застосування.

3.2. Захист інформації в комп'ютерних системах і мережах

3.2.1. Методи та засоби генерації та розподілу системних параметрів і ключів.

3.2.2. Захист інформації із використанням цифрового підпису та коду автентифікації.

3.2.3. Криптографічні методи та засоби захисту інформації в локальних та глобальних мережах.

3.2.4. Криптографічні протоколи встановлення ключів та оцінка їхньої якості.

3.2.5. Принципи забезпечення основних послуг - цілісності, конфіденційності, доступності й неспростовності в локальних та глобальних мережах.

3.2.6. Принципи побудування та функціонування інфраструктур з відкритими ключами, Порядок надання послуг з ЕЦП.

3.2.7. Протоколи шифрування на мережевому рівні та їх основні властивості і характеристики.

4. Захист інформації в інфокомунікаційних ситемах

4.1. Менеджмент інформаційної безпеки в інфокомунікаційних ситемах

4.1.1. Політики інформаційної безпеки.

4.1.2. Сертифікація систем управлніння кібербезпекою

4.1.3. Проектування, впровадження, моніторинг та удосконалення систем менеджменту інформаційної безпеки сучасних і перспективних інформаційно-комунікаційних систем.

4.1.4. Управління ризиками.

4.2. Методологія забезпечення інформаційної безпеки відповідно до 7-рівневої моделі BBC

4.2.1. Моделювання загроз кібербезпеки.

4.2.2. Локальні атаки в інфокомунікаційних мережах та їх типові сценарії.

4.2.3. Категорії мережевих атак, їх загальні сценарії та методи виявлення.

4.2.4. Віртуальні приватні мережі. Принципи побудови. Алгоритми та протоколи роботи.

4.2.5. Стандарти та протоколи захисту інформації у локальних мережах.

4.2.6. Стандарти та протоколи захисту інформації у системах електронної комерції.

4.2.7. Забезпечення безпечного віддаленого доступу до локальної мережі. Архітектура побудови та протоколи функціонування.

4.2.8. Технології, стандарти та протоколи забезпечення безпеки у безпроводових мережах.

4.3. Автоматизовані системи управління інформаційною безпекою

4.3.1. Методологія розробки безпечного програмного забезпечення

4.3.2. Методи захисту програмного коду від копіювання.

4.3.3. Сканери аналізу вразливостей. Архітектура побудови, принципи роботи.

4.3.4. Злоякісне програмне забезпечення. Загальні алгоритми розповсюдження, маскування.

4.3.5. Принципи побудови антивірусного програмного забезпечення

Рекомендована література

1. Виноградов И.М. Основы теории чисел.-М.: Наука, Главная редакция физико-математической литературы, 1981 – 176 с.
2. В. Столлингс. Криптография и защита сетей. Изд. «Вильямс». М. 2001. 669 с.
3. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Теорія. Практика. Застосування. – Харків: Форт, 2013. -880с.
4. А. Бессалов, А. Тележенко. Криптосистемы на эллиптических кривых. Киев. «Політехніка». 2004. – 224 с.
5. В. Задірака. О. Олексик. Комп'ютерна криптологія. Київ. – 2002. 502 с.
6. Б. Шнайер. Прикладная криптография. Протоколы, алгоритмы, исходные тексты та языке Си. – Москва. «Триумф». 2002. – 797с.
7. Бембо Мао. Современння криптографія. Теорія и практика. Москва. 2005.
8. Брюс Шнайер. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. Изд. Триумф. М., 2003 г. 815 с.
9. Свердлик М.Б. Оптимальные дискретные сигналы. М., «Советское радио», 1975, 200 с.
10. О.В. Вербицький. Вступ до криптології. – Львів, Видавництво науково-технічної літератури, 1998. – 247 с.
11. Введение в криптографию / Под общ. ред. В.В. Ященко. – М.: МЦНМО, «ЧеРо», 2001. – 286 с.
12. Барсуков В.С., Водолазкий В.В. Современные технологии безопасности. М.: «Нолидж», 2005. – 496 с., илл.
13. Мельников В.В. Защита информации в компьютерных системах. – М.: Финансы и статистика; Электронинформ, 2004. – 368 с.: ил.
14. Анин Б.Ю. Защита компьютерной информации. – СПб.: БХВ – Санкт-Петербург, 2006. – 384 с.: ил.

15. Поповский В.В., Персиков А.В. Основы криптографической защиты информации в телекоммуникационных системах, часть 1. Украина, Харьков, Компания СМИТ, 2010, 350 с.
16. Поповский В.В., Персиков А.В. Основы криптографической защиты информации в телекоммуникационных системах, часть 2. Украина, Харьков, Компания СМИТ, 2010, 294 с.
17. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях / Под ред. В.Ф. Шаньгина. – М.: Радио и связь, 1999. – 328 с.
18. Организация и современные методы защиты информации (под общей редакцией Диева С.А., Шаваева А.Г.). – М., Концерн «Банковский Деловой Центр», 1998, 472 с.
19. Методи захисту фінансової інформації: Навчальний посібник / В.К.Задірака, О.С.Олексюк. – К.: Вища шк., 2000. – 460 с.
20. Петров А.А. Компьютерная безопасность. Криптографические методы защиты. – М.: ДМК, 2006. – 448 с.: ил.
21. В. Ф. Шаньгин Информационная безопасность компьютерных систем и сетей. Серия: Профессиональное образование. Издательства: Форум, Инфра-М, 2008 г. Твердый переплет, 416 стр.
22. Квантовая криптография. Идеи и практика. Издательство: Белорусская наука, 2007 г. Мягкая обложка, 392 стр.
23. ISO/IEC 11700 -1,2.3 „Управління ключами”;
24. ISO/IEC 15946-1, 2,3 „ЦП , Протоколи встановлення ключів”;
25. ISO/IEC 9798-1,2,3,4,5. Протоколи автентифікації;
26. ISO/IEC 9797-1,2,3 Протоколи автентифікації;
27. ISO/IEC 13888-1.2.3. Неспростовність;
28. ISO/IEC 1488- 1.2.3. Схеми ЦП;
29. ISO/IEC 9594- 8 X-509 ITU Сертифікація відкритих ключів;
30. ISO/IEC 18031, 18032, 18033 – 1,2,3,4. Стандарти шифрування.

Основні сайти з інформацією відносно безпеки інформації

1. www.rsasecurity.com
2. www.nist.gov
3. www.eprint.iacr.org
4. www.citeseer.ist.psu.edu
5. www.ansi.org
6. www.cryptography.org
7. www.iso.org
8. www.linuxiso.org
9. www.cryptography.com
10. www.springerlink.com
11. www.cacr.math.uwaterloo.ca
12. www.financialcryptography.com
13. www.austinlinks.com
14. http://world.std.com/~franl/crypto.html
15. www.cryptonessie.org
16. www.cryptography.ru
17. www.osti.gov/eprints