МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ

ЗАТВЕРДЖУЮ
Голова приймальної
Комісії ХНУРЕ
_____ Валерій СЕМЕНЕЦЬ
«_29_» ____10____ 2021 р.

ПРОГРАМА
ФАХОВОГО ВСТУПНОГО ВИПРОБУВАННЯ
для вступу на 3 (освітньо-науковий) рівень вищої освіти
у 2022 році

Спеціальність 125 Кібербезпека

Протокол засідання приймальної комісії
№_21_ від _29.10_ 2021 р.

Голова предметної комісії _____ Геннадій ХАЛІМОВ
підпис (ім'я, прізвище)

Зав. відділом аспірантури
та докторантури _____ Володимир МАНАКОВ
підпис (ім'я, прізвище)

Відповідальний секретар
приймальної комісії _____ Аркадій СНІГУРОВ
підпис (ім'я, прізвище)

Харків 2021

Програма розроблена авторським колективом у складі: Халімов Г.З. – доктор технічних наук, професор (Харківський національний університет радіоелектроніки), Сєвєрінов О.В. – кандидат технічних наук, доценти (Харківський національний університет радіоелектроніки), Олейніков А.М. – кандидат технічних наук, професор (Харківський національний університет радіоелектроніки), Радівілова - доктор технічних наук, доцент (Харківський національний університет радіоелектроніки), Шумов О.І., технічний директор Приватного акціонерного товариства «Інститут інформаційних технологій».

ПРОГРАМА
вступного іспиту до аспірантури за спеціальністю 125 «Кібербезпека»

1. Спеціальні розділи математики

1.1. Основи теорії чисел

1.1.1. Поняття подільності чисел. Ділення із залишком. НСД двох чисел. Знаходження НСД двох чисел.

1.1.2. Прості числа. Великі прості числа.

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 математична статистика

1.3.1. Події та ймовірності, їх визначення та властивості. Приклади розподілів. Випадкові величини. Математичне очікування. Незалежні випадкові величини.

1.3.2. Основні поняття математичної 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 неблокові 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.

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.

2.1.8. Асиметричні 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. Електронний підпис і його реалізація. Оцінка ефективності електронних 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 електронного підпису в класі криптосистем Ель - Гамаля та порівняльний аналіз їх властивостей.

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

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

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

2.3. Технічний захист інформації.

2.4.1. Технічні канали витоку інформації. Радіоелектронні, вібро-акустичні та візуально-оптичні канали витоку інформації. Канали витоку інформації і їх структура та загальна характеристика. Сигнали як носії інформації. Способи і засоби отримання інформації по вібро-акустичному каналу. Лазерні системи акустичної розвідки (ЛСАР), їх структурна схема і принцип дії.

2.4.2. Методи та засоби захисту мовної інформації. Засоби протидії підслуховуванню: інформаційне приховування та енергетичне приховування. Класифікація технічних засобів закриття. Аналогове скремблювання: частотна інверсія, часова і частотна перестановка, цифрове шифрування.

2.4.3. Методи і радіотехнічні прилади запобігання витоку інформації за допомогою закладних приладів Демаскуючі признаки закладних приладів. Апаратно-програмні комплекси викриття, ідентифікації та локалізації радіоакустичних закладних пристроїв.

2.4.4. Основні характеристики і властивості радіоелектронного каналу витоку інформації. Джерела електромагнітних сигналів як носіїв інформації, їх властивості та особливості поширення. Побічні електромагнітні випромінювання технічних засобів.

2.4.5. Екранування та заземлення технічних засобів передачі інформації.

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

2.4.7. 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 ЕП та їх застосування.

3.1.5. Стандартні криптографічні протоколи розподілу таємниці. Властивості та реалізація.

3.1.6. Стандарти ґешування, 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 електронного підпису (ЕП) 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 ЕП.

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

4. Управління інформаційною безпекою

4.1. Системи аналізу вразливостей та принципи етичного хакінгу.

4.2. Методи виявлення та аналізу шкідливого програмного забезпечення.

4.3. Стандарти, протоколи та процедури, що відповідають за перевірку та управління безпекою продукту.

4.4. Загальні вимоги та підходи до розробки моделі загроз програмного забезпечення; патерни безпеки: керування ідентифікацією, автентифікація, моделі доступу, керування сесіями та ін.

4.5. Аспекти адміністрування, аудит та безпека інформаційних служб Internet.

4.6. Методи проведення цифрової криміналістики.

Критерії оцінювання знань вступника
при проведенні вступного іспиту

Задовільно, E (60-65): знання основ теоретичного програмного матеріалу за питаннями екзаменаційного білету. Відсутні загальні висновки, наявність некоректно представленого матеріалу, наявність великої кількості семантичних, стилістичних недоліків та помилок.

Задовільно, D (66-74): знання основ навчально-програмного матеріалу в обсязі, необхідному для подальшого навчання, за питаннями екзаменаційного білету. Присутні загальні обґрунтовані висновки, наявність некоректно представленого матеріалу, наявність семантичних, стилістичних недоліків та помилок.

Добре, C (75-80): повне знання програмного теоретичного матеріалу, розкриття питань екзаменаційного білету. Наявність некоректно представленого матеріалу, наявність семантичних, стилістичних недоліків та помилок, наведені стислі неповні висновки.

Добре, C (81-89): повне знання програмного теоретичного матеріалу, системний характер знань з дисципліни, розкриття питань екзаменаційного білету. Наведені розгорнуті висновки, але є наявність некоректно представленого матеріалу, наявність семантичних, стилістичних недоліків та помилок.

Відмінно, B (90-95): глибокі, систематизовані знання теоретичного програмного матеріалу, повне розкриття та обґрунтування відповідей на питання екзаменаційного білету. Наведення повних розгорнутих висновків, але є наявність некоректно представленого матеріалу, наявність семантичних, стилістичних недоліків та помилок.

Відмінно, A (96-100): всебічні, глибокі, систематизовані знання та логічне трактування теоретичного програмного матеріалу, повне розкриття та обґрунтування відповідей на питання екзаменаційного білету. Наведення

повних розгорнутих висновків та відсутність семантичних, стилістичних помилок, коректно та грамотно представлений матеріал.

Шкала оцінювання: національна та ЄКТС

Оцінка з дисципліни	Оцінка ЄКТС	Оцінка за національною шкалою
96-100	A	5 (відмінно)
90-95	B	5 (відмінно)
75-89	C	4 (добре)
66-74	D	3 (задовільно)
60-65	E	3 (задовільно)
35-59	FX	2 (незадовільно)
1-34	F	

Рекомендована література

1. Антіпов І.Є., Олейніков А.М., Ликов Ю.В., Кукуш В.Д., Милютченко І.О. Засоби та системи технічного захисту інформації. Навчальний посібник для студентів ЗВО // Харків: ФОП Панов А.М., 2019. – 216 с.

2. Богуш В.М. Інформаційна безпека держави: [навч. посіб.] / В.М. Богуш, О.К. Юдін. – К.: МК-Прес, 2005. – 432 с.

3. Гончарова Л.Л., Возненко А.Д., Стасюк О.І., Коваль Ю.О. Основи захисту інформації в телекомунікаційних та комп'ютерних мережах. – К.: ДЕТУТ, 2013. – 435 с.

4. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія: Теорія. Практика. Застосування: Підручник для вищих навчальних закладів. – Харків: Видавництво «Форт», 2013. – 880 с.

5. Горбенко Ю.І. Побудування та аналіз систем, протоколів і засобів криптографічного захисту інформації: монографія. - Частина 1: Методи побудування та аналізу, стандартизація та застосування криптографічних систем / За зат. ред. д.т.н., професора І.Д. Горбенка. – Харків : Видавництво «Форт», 2015. – 960 с.

6. Задірака В., Олексик О. Комп'ютерна криптологія. - Київ, 2002. - 502 с.

7. Замула О.А. Нормативно–правове забезпечення інформаційної безпеки. Комплексні системи захисту інформації: навч. посібник. / О.А. Замула, Ю.І. Горбенко, О.І. Шумов. – Харків: ХНУРЕ, 2010. – 248 с.

8. Кібербезпека мереж наступного покоління : навч. посіб. / О.О. Вараксін, Є. В. Васіліу, С. М. Горохов и др. ; за ред. В. Г Кононовича ; М-во освіти і науки України, Одеська нац. академія зв'язку ім. О. С. Попова. – Одеса : ОНАЗ ім. О. С. Попова, 2013. – 240 с.

9. Конспект лекцій з дисципліни «Безпека безпроводових мереж» для студентів усіх форм навчання спеціальності 125 «Кібербезпека» освітньої

програми «Безпека інформаційних і комунікаційних систем» [Електронний ресурс] / упоряд.: О.В. Сєвєрінов, О.І. Федюшин, А.В. Власов. – Електронне видання. – Харків: ХНУРЕ, 2019. – 118 с. - pdf / 2,32 Mb.

10. Конспект лекцій з дисципліни «Методи захисту децентралізованих систем» для студентів усіх форм навчання спеціальності 125 «Кібербезпека» освітньої програми «Безпека інформаційних і комунікаційних систем» [Електронний ресурс] / упоряд.: А.В. Власов., О.В. Сєвєрінов, М.О. Шафоростов. – Електронне видання. – Харків: ХНУРЕ, 2021. – 240 с. - pdf / 8,5 Mb.

11. І.Д. Горбенко, Т.О. Гріненко. Захист інформації в інформаційно-телекомунікаційних системах: Навч. Посібник. Ч. 1. Криптографічний захист інформації. – Харків: ХНУРЕ, 2004. – 368 с.

12. Кузнецов О.О. Потокові шифри: монографія / О.О. Кузнецов, О.В. Потій, М.О. Полуяненко, Ю.І. Горбенко; за загальною редакцією І.Д. Горбенко. – Харків: Видавництво «Форт», 2019. – 544 с.

13. Кузнецов О.О. Протоколи захисту інформації у комп'ютерних системах та мережах: навч. посібник / О.О. Кузнецов, С.Г. Семенов; МОН України, ХНУРЕ. – Харків: ХНУРЕ, 2009. – 184 с.

14. Методи захисту фінансової інформації: Навчальний посібник / В.К. Задірака, О.С. Олексюк. – К.: Вища шк., 2000. – 460 с.

15. Олейніков А.М. Методи та засоби захисту інформаці. Навчальний посібник для студентів вищих навчальних закладів // Харків: НТМТ , 2014. – 298 с.

16. Поповский В. В., Персиков А. В. Основы криптографической защиты информации в телекоммуникационных системах: [учеб. изд.]. Ч.2. – Харьков: СМИТ, 2010. – 296 с.

17. Поповський В.В., Пастушенко Н.С., Стрелковская И.В., Сабурова С.А. Методы научных исследований в телекоммуникациях: учеб. пособие: в 2-х т. Т.2/ под ред. В.В. Поповського. – Х.: СМИТ, 2013. – 330 с.

18. Сенів М.М. Безпека програм та даних: навч. посіб. / М.М. Сенів,

В.С. Яковина; М-во освіти і науки України, Нац. ун-т "Львівська політехніка". – Львів: Вид-во Львівськой політехніки, 2015. – 256 с.

19. Теорія інформації: підручник для слухачів, курсантів та студентів вищих навчальних закладів / І.В. Рубан, С.І. Хмелевський, О.В. Сєвєрінов та ін. – Харків: ХНУПС, 2018. – 276 с.

20. Тимошенко Л.П. Схемотехніка пристроїв технічного захисту інформації: навч. посіб. [Ч.1] / Л.П. Тимошенко; за ред. В.М. Карташова. – Харків: СМІТ, 2012. – 340 с.

21. ISO/IEC 11700-1, 2, 3. Information technology - Security techniques - Key management.

22. ISO/IEC 15946-1, 2, 3. Information technology - Security techniques - Cryptographic techniques based on elliptic curves.

23. ISO/IEC 9798-1, 2, 3, 4, 5. IT Security techniques - Entity authentication.

24. ISO/IEC 9797-1, 2, 3. Information technology - Security techniques - Message Authentication Codes (MACs).

25. ISO/IEC 13888-1.2.3. Information security — Non-repudiation.

26. ISO/IEC 14888- 1.2.3. IT Security techniques — Digital signatures with appendix.

27. ISO/IEC 9594-8. Information technology - Open Systems Interconnection - The Directory - Part 8: Public-key and attribute certificate frameworks.

28. ISO/IEC 18031. Information technology - Security techniques - Random bit generation.

29. ISO/IEC 18032. Information technology - Security techniques - Prime number generation.

30. ISO/IEC 18033 – 1, 2, 3, 4. Information technology - Security techniques - Encryption algorithms.

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.osti.gov/eprints.