Національний технічний університет
“Харківський політехнічний інститут”

ЗАГАЛЬНА ПРОГРАМА

Докторського іспиту зі спеціальності

Галузь знань 12 “Інформаційні технології”
Спеціальність 125 “Кібербезпека та захист інформації”

Затверджено вченою радою
Навчально-наукового інституту
Комп’ютерних наук та інформаційних
технологій

Протокол № 02 від “ 21 ” лютого 2023 р.

Директор Михайло ГОДЛЕВСЬКИЙ

Харків 2023

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. Загальна програма докторського іспиту зі спеціальності аспірантів складена відповідно до Положення про підготовку здобувачів вищої освіти ступеня доктора філософії в аспірантурі Національного технічного університету “Харківський політехнічний інститут”, Положення про докторський іспит зі спеціальності та освітньо-наукової програми спеціальності 125 – Кібербезпека та захист інформації.

2. ЗМІСТ ПРОГРАМИ

1. Спеціальні розділи математики

   1.1 Основи теорії чисел.
   1.2 Основи теорії груп, кілець та полів.
   1.3 Еліптичні криві, визначення та властивості.
   1.4 Теорія ймовірності та математична статистика.
   1.5 Математичні основи теорії інформації.
   1.6 Алгоритмічні основи криптографії.

2. Методи та засоби захисту інформації. Криптографічні системи
   2.1 Основи теорії захисту інформації.
   2.2 Основні функції криптографічних систем.
   2.3 Проектування та використання систем і засобів захисту інформації.
   2.4 Технічний захист інформації.
   2.5 Системи керування захистом інформації.

3. Захист інформації в системах і мережах
   3.1 Основні положення безпеки інформації.
   3.2 Захист інформації в комп’ютерних системах і мережах.
   3.3 Методи та засоби генерації та розподілу системних параметрів і ключів.

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

4.6.Методи проведення цифрової криміналістики.

5. Математичне моделювання систем безпеки

5.1 Принципи побудови математичних моделей.
5.2 Математичні основи моделей безпеки.
5.3 Моделі з дискреційним управлінням доступу.
5.4 Моделі ізольованого програмного середовища.
5.5 Моделі з мандатним управлінням доступу.
5.6 Моделі безпеки інформаційних потоків.
5.7 Моделі рольового управління доступом.

6. Захист інформації в децентралізовани системах

6.1Централізовані та децентралізовані мережі.
6.2 Технологія блокчейн.
6.3 Технології майнінга.
6.4 Основи смарт-контрактів.

Рекомендована література

1. Кузнецов О.О., Євсеєв С.П., Кавун С.В., та Король О.Г. Сигнали і коди. Алгебраїчні методи синтезу. Монографія. Харків, Україна: Вид. ХНЕУ, 2009.
2. Кузнецов О.О., Євсеєв С.П., та Кавун С.В. Захист інформації та економічна безпека підприємства. Монографія. Харків, Україна: Вид. ХНЕУ, 2009.
3. 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.
4. Кузнецов О.О., Євсеєв С.П., Король О.Г. Захист інформації в ІС. Харків: Вид. ХНЕУ, 2011. –510 с.
5. Ленков С. В., Перегудов Д. А., и Хорошко В. А., *Методы и средства защиты информации : монография* [в 2-х т.] Т. 2. Информационная безопасность. К. : Арий, 2008.
6. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія: Теорія. Практика. Застосування: Підручник для вищих навчальних закладів. – Харків: Видавництво “Форт”, 2013. – 880 с.
7. 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.

8. Євсеєв С.П. Кібербезпека: сучасні технології захисту. / Євсеєв С.П, Остапов С.Е., Король О.Г. // Навчальний посібник для студентів вищих навчальних закладів. Львів: “Новий Світ- 2000”, 2019. – 678.

9. Євсеєв С.П., Йохов О.Ю., та Король О.Г. Гешування даних в інформаційних системах. Монографія. Харків, Україна: Вид. ХНЕУ, 2013.

10. Задірака В., Олексик О. Комп’ютерна криптологія. – Київ, 2002. – 502 с.

11. 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.

12. 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.

13. 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 Львівської політехніки, 2015. – 256 с.

14. Edited by Serhii Yevseiev, Volodymir Ponomarenko, Oleksandr Laptiev, Oleksandr Milov. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p.

15. Hryshchuk R., Construction methodology of information security system of banking information in automated banking systems : monograph / R. Hryshchuk, S. Yevseiev, A.Shmatko //– Vienna.: Premier Publishing s. r. o., 2018. – 284 p.

16. ISO/IEC 27000:2018. Information technology – Security techniques – Information security management systems – Overview and vocabulary. URL: https://www.iso.org/standard/73906.html

17. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements. URL: https://www.iso.org/standard/82875.html

18. ISO/IEC IS 27006:2015 – Requirements for bodies providing audit and certification of information security management systems. URL: https://www.iso.org/standard/62313.html

19. ISO/IEC IS 27002:2013 – Code of practice for information security controls. URL: https://www.iso.org/standard/54533.html.

20. ISO/IEC 27003:2017. Information technology – Security techniques – Information security management systems – Guidance. URL: https://www.iso.org/standard/63417.html.

21. ISO/IEC 27004:2016. Information technology – Security techniques – Information security management – Monitoring, measurement, analysis and

evaluation. URL: https://www.iso.org/standard/64120.html

22. ISO/IEC 27007:2020. Information security, cybersecurity and privacy protection – Guidelines for information security management systems auditing. URL: https://www.iso.org/standard/77802.html

23. ISO/IEC TR 27008:2011 – Guidance for auditors on ISMS controls. URL: https://www.iso.org/standard/45244.html.

24. SO/IEC 27013:2021. Information security, cybersecurity and privacy protection – Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1. URL: https://www.iso.org/standard/78752.html.

25. ISO/IEC 27014: 2020. Information security, cybersecurity and privacy protection – Governance of information security. URL: https://www.iso.org/standard/74046.html

26. ISO/IEC 27010:2015. Information technology – Security techniques – Information security management for inter-sector and inter-organizational communications. URL: https://www.iso.org/standard/68427.html

27. ISO/IEC 27011:2016. Information technology – Security techniques – Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations. URL: https://www.iso.org/standard/64143.html

28. ISO/IEC TR 27015:2012. Information technology – Security techniques – Information security management guidelines for financial services. URL: https://www.iso.org/standard/43755.html

29. ISO/IEC 27031:2011. Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity. URL: https://www.iso.org/standard/44374.html.

30. ISO/IEC 27033-1:2015. Information technology – Security techniques – Network security – Part 1: Overview and concepts. URL: https://www.iso.org/standard/63461.html.

31. ISO/IEC 27034-6:2016. Information technology – Security techniques – Application security – Part 6: Case studies. URL: https://www.iso.org/standard/60804.html.

32. ISO/IEC 27034-6:2016. Information technology – Security techniques – Application security – Part 5: Protocols and application security controls data structure. URL: https://www.iso.org/standard/55585.html.

33. ISO/IEC 27037:2012 Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence. URL: https://www.iso.org/search.html?q=ISO/IEC%2027037.

34. ISO/IEC 15408-2:2022. Information security, cybersecurity and privacy protection – Evaluation criteria for IT security – Part 2: Security functional components. URL: https://www.iso.org/standard/72892.html.

35. ISO/IEC 15408-3:2022. Information security, cybersecurity and privacy protection – Evaluation criteria for IT security – Part 3: Security assurance components. URL: https://www.iso.org/standard/72906.html.

36. ISO/IEC 15408-4:2022. Information security, cybersecurity and privacy

protection – Evaluation criteria for IT security – Part 4: Framework for the specification of evaluation methods and activities. URL: https://www.iso.org/standard/72913.html.

37. ISO/IEC 17799:2005/Cor 1:2007. Information technology – Security techniques – Code of practice for information security management – Technical Corrigendum 1. URL: https://www.iso.org/standard/46381.html.

38. ISO/IEC 10181-1:1996. Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview. URL: https://www.iso.org/standard/24404.html

39. ISO/IEC 10181-2:1996. Information technology – Open Systems Interconnection – Security frameworks for open systems: Authentication framework. URL: https://www.iso.org/standard/18198.html.

40. ISO/IEC 10181-3:1996. Information technology – Open Systems Interconnection – Security frameworks for open systems: Access control framework. URL: https://www.iso.org/standard/18199.html.

41. Бобало Ю.Я., Горбатий І.В. (ред.) Інформаційна безпека. Навчальний посібник. – Львів : Видавництво Львівської політехніки, 2019. – 580 с.

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

43. Бурячок В.Л., Грищук Р.В., та Хорошко В.О., під заг. ред. проф. В. О. Хорошка, “Політика інформаційної безпеки”, ПВП “Задруга”,. 2014.

44. Грищук Р.В., та Даник Ю.Г. Основи кібернетичної безпеки: Монографія /; за заг. ред. Ю. Г. Данника. Житомир: ЖНАЕУ, 2016.

45. Юдін О.К. “Інформаційна безпека. Нормативно-правове забезпечення”, К.: НАУ, 2011.

46. 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.

47. Математичне моделювання телекомунікаційних систем та мереж: навчальний посібник [Текст] / Є.М. Чернихівський. – Львів: Видавництво Львівської політехніки, 2011. – 272 с

48. Махней О. В. Математичне моделювання : навчальний посібник / О. В. Махней. – Івано-Франківськ : Супрун В. П., 2015. – 372 с.

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

50. Кравченко П., Скрябін Б. Блокчейн та децентралізовані системи. Ч. 1. Харків: Промарт, 2018. – 400 с.

51. Кравченко П. Блокчейн і децентралізовані системи. Ч. 2 – Харків: ПРОМАРТ, 2019. – 452 с.

52. Кравченко П. Блокчейн і децентралізовані системи. Ч. 3 – Харків:

ПРОМАРТ, 2020. – 306 с.

53. 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.

Перелік запитань

1. Поняття подільності чисел. Ділення із залишком.
2. Прості числа. Великі прості числа. Методи побудови “великих” простих чисел.
3. Функція Ейлера. Узагальнена функція Ейлера. Визначення та головні властивості.
4. Групи, головні поняття та визначення.
5. Мультиплікативні групи.
6. Підстановки. Групи підстановок.
7. Підгрупи.
8. Кільця, визначення та властивості. Кільце з одиницею. Ізоморфні кільця.
9. Поля, визначення та властивості. Прості та поширені поля.
10. Еліптичні криві, визначення та властивості.
11. Дискретно- ймовірнісний простір.
12. Події та ймовірності, їх визначення та властивості.
13. Випадкові величини. Мат. очікування. Незалежні випадкові величини.
14. Закони розподілу ймовірностей. Біноміальний, показовий, рівномірний та нормальний розподіл.
15. Перевірка статистичних гіпотез.
16. Схема іспитів Бернуллі, критерій знаків для однієї вибірки.
17. Критерій згоди Колмогорова, x^2 – квадрат Пірсона.
18. Умовна та безумовна ентропія.
19. Умовна апостеріорна ентропія.
20. Середня взаємна інформація.
21. Блокові та неблокові коди.
22. Норми, метрики та кодові відстані.
23. Лінійні коди, згорткові коди, збиткові коди.
24. Псевдовипадкові послідовності.
25. Лінійні та нелінійні рекурентні послідовності, їх властивості.
26. Основні методи обчислень в багатослівній арифметиці та оцінка їх складності.
27. Методи побудування “великих” простих чисел та незвідних поліномів, складність та реалізація алгоритмів.
28. Афінний та проективний базиси скалярного множення в групі точок еліптичних кривих.

29. Методи побудування системних параметрів для криптографічних додатків на еліптичних кривих.
30. Методи розв’язку дискретних логарифмічних рівнянь в групі точок еліптичних кривих та порівняльна оцінка їх складності
31. Моделі загроз та порушника.
32. Фактори уразливості та канали витоку інформації, шляхи несанкціонованого доступу.
33. Концепція захищеної комп'ютерної системи (мережі).
34. Політики безпеки інформації та їх впровадження.
35. Основні функції криптографічних систем.
36. Криптографія та криптографічний аналіз.
37. Класифікація криптографічних систем по стійкості.
38. Теоретично недешифруємі системи й умови їх реалізації.
39. Обчислювально-стійкі та доказово стійкі системи й умови їхньої реалізації.
40. Інформаційні характеристики джерел повідомлень, криптограм і ключів.
41. Класифікація шифрів. Симетричні та несиметричні алгоритми шифрування.
42. Блокові та потокові алгоритми шифрування, та їх властивості.
43. Генератори псевдовипадкових послідовностей.
44. Несиметричні алгоритми шифрування та їх властивості.
45. Умови реалізації та галузі застосування систем шифрування.
46. Автентифікація. Погрози порушення автентичності.
47. Модель взаємної довіри, взаємної недовіри та взаємного захисту.
48. Методи автентифікації в потокових системах шифрування, оцінка їх ефективності.
49. Цифровий підпис, оцінка ефективності електронних підписів.
50. Класифікація методів криптографічного аналізу та умови здійснення.
51. Класифікація та характеристика симетричних криптографічних систем. Основні вимоги та склад симетричних криптографічних систем.
52. Основні принципи та режими симетричного шифрування.
53. Класифікація та характеристика несиметричних криптографічних систем.
54. Основні протоколи встановлення таємниці та ключів.
55. Алгоритми цифрового підпису та порівняльний аналіз їх властивостей.
56. Алгоритм цифрового підпису в групі точок еліптичних кривих.
57. Криптографічна стійкість та складність перетворень.
58. Класифікація, суть та порівняльний аналіз стандартних алгоритмів та засобів гешування.
59. Нормативна база, яка визначає процеси розробки та створення комплексних систем захисту інформації.
60. Вимоги до перспективних симетричних криптографічних систем.
61. Стандарти симетричного блокового шифрування. Стійкість симетричних

блокових криптосистем.

62. Розробка програмних і апаратних засобів криптографічного захисту інформації. Основні вимоги. Принципи програмної та апаратної реалізації.
63. Інфраструктури відкритих ключів, призначення, вимоги та принципи функціонування.
64. Комплексні системи захисту центрів сертифікації ключів, вимоги до них, порядок створення і застосування.
65. Технічні канали витоку інформації. Радіоелектронні, вібро-акустичні та візуально-оптичні канали витоку інформації.
66. Канали витоку інформації і їх структура та загальна характеристика.
67. Сигнали як носії інформації.
68. Способи і засоби отримання інформації по вібро-акустичному каналу.
69. Лазерні системи акустичної розвідки (ЛСАР), їх структурна схема і принцип дії.
70. Методи та засоби захисту мовної інформації. Засоби протидії підслуховуванню: інформаційне приховування та енергетичне приховування.
71. Класифікація технічних засобів закриття.
72. Аналогове скремблювання: частотна інверсія, часова і частотна перестановка, цифрове шифрування.
73. Методи і радіотехнічні прилади запобігання витоку інформації за допомогою закладних приладів.
74. Демаскуючі признаки закладних приладів.
75. Апаратно-програмні комплекси викриття, ідентифікації та локалізації радіоакустичних закладних пристроїв.
76. Основні характеристики і властивості радіоелектронного каналу витоку інформації.
77. Джерела електромагнітних сигналів як носіїв інформації, їх властивості та особливості поширення.
78. Побічні електромагнітні випромінювання технічних засобів. Екранування та заземлення технічних засобів передачі інформації.
79. Вимоги та методи забезпечення захисту інформації від витоку по технічним каналам в АС 1 та АС2.
80. Вимоги нормативних документів та захист електронних засобів інформаційно- телекомунікаційних систем від зовнішнього впливу.
81. Архітектура системи безпеки операційних систем (ОС).
82. Диспетчер облікових записів (ДОЗ).
83. Паролі, відновлення паролів.
84. Захист файлів і компоненти (NTFS).
85. Права доступу. Дозволи NTFS.
86. Захист реєстру. Інформація про безпеку реєстру. Захист від локального та віддаленого доступу. Аудит реєстру.
87. Основні положення безпеки інформації.

88. Сутність вимог основних стандартів по забезпеченню безпеки інформації.
89. Призначення та ціль розробки стандарту. Етапи розробки стандартів.
90. Порядок сертифікації засобів захисту.
91. Основні вимоги стандартів по управлінню ключами. Функції центрів управління та сертифікації ключів.
92. Стандарти ЦП та їх застосування.
93. Стандартні криптографічні протоколи розподілу таємниці. Властивості та реалізація.
94. Стандарти гешування, властивості та застосування.
95. Методи та засоби генерації та розподілу системних параметрів і ключів.
96. Захист інформації із використанням цифрового підпису та коду автентифікації.
97. Криптографічні методи та засоби захисту інформації в локальних та глобальних мережах.
98. Криптографічні протоколи встановлення ключів та оцінка їх якості.
99. Принципи забезпечення основних послуг – цілісності, конфіденційності, доступності й автентичності в локальних та глобальних мережах.
100. Принципи побудування та функціонування інфраструктур з відкритими ключами.
101. Порядок надання послуг з ЦП.
102. Протоколи шифрування на мережевому рівні та їх основні властивості і характеристики.
103. Системи аналізу вразливостейю
104. Принципи етичного хакінгу.
105. Методи виявлення та аналізу шкідливого програмного забезпечення.
106. Стандарти, протоколи та процедури, що відповідають за перевірку та управління безпекою продукту.
107. Загальні вимоги та підходи до розробки моделі загроз програмного забезпечення; патерни безпеки: керування ідентифікацією, автентифікація, моделі доступу, керування сесіями та ін.
108. Аспекти адміністрування, аудит та безпека інформаційних служб Internet.
109. Методи цифрової криміналістики.

110. Принципи побудови математичних моделей. Основні види моделювання.
111. Формальні методи побудови моделей: кібернетичний підхід, системна динаміка, теоретично- множинний підхід.
112. Ідентифікація параметрів математичної моделі.
113. Адекватність, чутливість, непротирічність моделі.
114. Основні види формальних моделей безпеки.
115. Проблема адекватності реалізації моделі безпеки в реальному комп’ютерній системі.

116. Моделі з дискреційним управлінням доступу.
117. Модель матриці доступив Харрісона-Руззо-Ульмана. Опис моделі. Аналіз безпеки систем ХРУ.
118. Модель типизированной матриці доступив.
119. Модель поширення прав доступу Take-Grant. Основні положення класичної моделі Take-Grant. Розширена модель Take-Grant. Подання систем Take-Grant системами ХРУ.
120. Дискреційні ДП-моделі. Базова ДП-модель. ДП-модель без кооперації довірених і недовірених суб'єктів.
121. Суб'єктно- орієнтована модель ізольованого програмного середовища.
122. Коректність суб'єктів в ДП-моделях КС з дискреційним управлінням доступом.
123. ДП- модель з функціонально асоційованими з суб'єктами сутностями.
124. ДП-модель для політики безпечного адміністрування.
125. ДП-модель для політики абсолютного поділу адміністративних і призначених для користувача повноважень.
126. ДП-модель з функціонально або параметрично асоційованими з суб'єктами сутностями.
127. Застосування ФАС ДП-моделі для аналізу безпеки веб-систем.
128. Моделі з мандатним управлінням доступу. Модель Бела-ЛаПадули.
129. Модель мандатної політики цілісності інформації Віба.
130. Модель систем військових сполучень. Загальні положення та основні поняття.
131. Неформальне опис моделі СВС. Формальний опис моделі СВС.
132. Моделі безпеки інформаційних потоків.
133. Автоматна модель безпеки інформаційних потоків.
134. Програмна модель контролю інформаційних потоків. Імовірнісна модель безпеки інформаційних потоків.
135. ДП-моделі безпеки інформаційних потоків за часом. ДП-модель з блокуючими доступами довірених суб'єктів.
136. Мандатна ДП-модель з блокуючими доступами довірених суб'єктів.
137. Мандатна ДП-модель з ототожненням породжених суб'єктів.
138. Базова модель рольового управління доступом.
139. Модель адміністрування рольового управління доступом. Основні положення.
140. Адміністрування множин авторизованих ролей користувачів.
141. Адміністрування множин прав доступу, якими володіють ролі.
142. Адміністрування ієрархії ролей.
143. Модель мандатної рольового управління доступом.
144. Захист від загрози конфіденційності інформації.
145. Захист від загроз конфіденційності та цілісності інформації.
146. Мандатна сутнісно- рольова ДП-модель управління доступом та інформаційними потоками в операційних системах сімейства Linux.

147. Централізовані та децентралізовані мережі.
148. Технологія блокчейн.
149. Технології майнінга.
150. Моделі знаходження консенсусу.
151. Криптографічні протоколи гешування.
152. Основи смарт-контрактів. Принципи формування смарт-контрактів.
153. Принципи токенізації.
154. Принципи формування та особливості Bitcoin Script.
155. Принципи формування протоколу Bitshares.
156. Формування SmartCoins.
157. Облікова система Atomic Swap.
158. Принципи створення Stablecoin.
159. Проведення транзакцій та формати ключів у BitCoin.

Затверджено на засіданні кафедри “Кібербезпека”

від “ 06 ” лютого 2023 р. протокол № 10 .

Завідувач кафедри _____ Сергій ЄВСЕЄВ

Гарант програми _____ Сергій ЄВСЕЄВ