МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧЕРНІВЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
імені Юрія Федьковича
Навчально-науковий інститут фізико-технічних та комп'ютерних наук

Кафедра *радіотехніки та інформаційної безпеки*

ЗАТВЕРДЖУЮ

Ректор _____ Роман ПЕТРИШИН

«____» _____ 2023 року

ПРОГРАМА ВСТУПНОГО КОМПЛЕКСНОГО ФАХОВОГО ІСПИТУ

на навчання за рівнем вищої освіти магістр
на базі рівня вищої освіти бакалавр

Спеціальність ***125 Кібербезпека та захист інформації***
(шифр і назва спеціальності)

Освітньо-професіна програма ***Кібербезпека***
(назва ОП)

Схвалено
Вченою радою ННІФТКН
протокол № 2 від 30.03.2023 р.

Голова Вченої ради О.В. Ангельський О.В.

Чернівці 2023 рік

ПРОГРАМА ДЛЯ ВСТУПНИКІВ
на здобуття кваліфікаційного рівня *"Магістр"*
спеціальність «Кібербезпека та захист інформації»
Навчально- науковий інститут фізико-технічних та комп'ютерних наук.
Кафедра радіотехніки та інформаційної безпеки

1. Лінійні блокові систематичні коди, генеруюча та перевіркова матриця.
2. Характеристики мовних сигналів.
3. Основні методи закриття мовної інформації.
4. Циклічні коди.
5. Методи вимірювання акустичних параметрів.
6. Аналогові скремблери: класифікація та принцип дії.
7. Згорткові коди.
8. Акустичні вимірювальні перетворювачі.
9. Цифрові скремблери: класифікація та принцип дії.
10. Імпульсно-кодова модуляція.
11. Ентропія дискретного джерела повідомлень. Умовна та сумісна ентропія зв'язаних джерел повідомлень.
12. Власна інформація повідомлень.
13. Сумісна та взаємна інформація повідомлень.
14. Взаємна інформація зв'язаних каналом джерел повідомлень. Кількість інформації, що передається по каналу зв'язку.
15. Загальні принципи акустичних перетворювачів. Механічні та електричні аналогії в акустиці.
16. Стабілізація частоти радіопередаючих пристроїв.
17. Вимоги до систем передавання інформації в реальному часі.
18. Акустоелектроніка. П'єзоелектричні резонатори. Пристрої на поверхневих акустичних хвилях.
19. Амплітудна модуляція. Модуляція на керуючу сітку.
20. Імпульсна та перехідна характеристики лінійних дискретних систем.
21. Види ліній зв'язку та їх основні характеристики.
22. Анодна амплітудна модуляція.
23. Властивості лінійних дискретних систем.
24. Первинні та вторинні параметри ліній зв'язку.
25. Генератори з зовнішнім збудженням.
26. Пряме та обернене перетворення Фур'є для дискретних сигналів.
27. Поверхневий ефект в лініях зв'язку. Причина явища.
28. Види і природа виникнення каналів витоку інформації при експлуатації ЕОМ.
29. Властивості z-перетворень.
30. Ефект близькості (зближення) в лініях зв'язку. Причина явища.
31. Джерела утворення радіоканалів витоку інформації.
32. Передавальна функція лінійних дискретних систем.
33. Конструктивні елементи кабелів зв'язку.
34. Класифікація технічних каналів витоку інформації.
35. Основні класи симетричних криптосистем.
36. Основні етапи синтезу електричних фільтрів. Синтез НЧ-фільтра за Батервортом.

37. Принцип дії пасивного інфрачервоного датчика руху.
38. Модель криптосистеми з відкритим ключем.
39. Вплив паралельного від'ємного оберненого зв'язку за напругою на коефіцієнт підсилення.
40. Загальна модель системи захисту об'єкту.
41. Шифр Віженера.
42. Вплив послідовного від'ємного (додатного) оберненого зв'язку за напругою на коефіцієнт підсилення.
43. Типи датчиків, які використовуються в системі протипожежного захисту.
44. Шифр Хілла.
45. Вплив послідовного від'ємного оберненого зв'язку за напругою на вхідний опір.
46. Класифікація протикрадіжкових систем захисту.
47. Поліграмні шифри.
48. Вплив місцевого та загального оберненого зв'язку на відносну зміну коефіцієнту підсилення за напругою у випадку двокаскадного підсилювача.
49. Основні складові базової системи відеоспостереження.
50. Алгоритм шифрування DES (Data Encryption Standard).
51. Вхідні кола засобів приймання та обробки інформації. Випадок ємнісного та індуктивного зв'язку з антеною.
52. Абсолютна і відносна похибки вимірювання. Приведена похибка. Систематичні і випадкові похибки.
53. Криптосистема RSA (Ronald Linn Rivest, Adi Shamir, Leonard Adleman).
54. Переваги та недоліки приймачів супергетеродинного типу. Структурна схема супергетеродинного приймача.
55. Резонансні явища в колах синусоїдального струму. Резонанс напруг і резонанс струмів.
56. Криптосистема Ель-Гамаля.
57. Переваги та недоліки приймачів прямого підсилення. Структурна схема приймача прямого підсилення.
58. Перехідні процеси. Закони комутації. Методи розрахунку перехідних струмів та напруг.
59. Криптосистема Рабіна.
60. Фазові детектори, їх типи, основні характеристики та схемотехнічна реалізація.
61. Реактивні електричні фільтри. Умови пропускання сигналу.
62. Поняття про цифровий підпис.
63. Параметри і характеристики детекторів ЧМ коливань. Основні методи детектування ЧМ коливань. Детектори ЧМ коливань із взаєморозналагодженними контурами.
64. Централізована й децентралізована обробка інформації в інформаційно-вимірювальних комплексах.
65. Основні види модуляції. Амплітудна модуляція.
66. Параметри радіоелектронних засобів та їх вплив на електромагнітну сумісність.
67. Нормальний закон розподілу випадкової похибки. Середньо-квадратичне значення та дисперсія випадкової похибки.
68. Спектральний метод аналізу проходження детермінованих радіосигналів через лінійні кола.
69. Структура електромагнітного поля та принципи екранування.

70. Мостовий метод вимірювання параметрів. Повне рівняння балансу моста. Схеми вимірювання R, C, L, Q, tgδ.
71. Динамічні системи, умова стійкості.
72. Індустріальні джерела завад.
73. Розрахунок коефіцієнта корисної дії антенного фідера.
74. Будова систем цифрової обробки сигналів.
75. Побічні випромінювання. Електромагнітне екранування.
76. Способи вимірювання частоти. Вимірювання частоти і часових інтервалів методом калібровочних міток.
77. Етапи перетворення аналогового сигналу в цифровий.
78. Стеки. Типи стеків, призначення.
79. Типи архітектур мікропроцесорних систем.
80. Малі рамкові (магнітні) антени без магнітодіелектричного осердя.
81. Подавлення шумів. Синхронна фільтрація.
82. Гарвардська та Прінстонська архітектури мікропроцесорних систем.
83. Канали зв'язку в інформаційно- вимірювальних системах.
84. Послідовність операцій аналогово-цифрового перетворення сигналів.
85. Професійні системи рухомого радіозв'язку. Транкінговий зв'язок.
86. Шуми антен. Формула Найквіста для антен.
87. Дискретизація сигналу по часу. Дискретний сигнал. Квантований сигнал. Цифровий сигнал.
88. IP-телефонія в системах зв'язку третього покоління.
89. Різновиди інформаційно-вимірювальних систем.
90. Криптографічні хеш-фунції.
91. Електричне коло: визначення, структурні елементи, основні закони.
92. Види і склад інформаційно-вимірювальних комплексів.
93. Спектри амплітудно-модульованих коливань.
94. Повітряні та екрановані фідерні лінії.
95. Синхронний і асинхронний режими організації передавання.
96. Динамічне представлення сигналів за допомогою дельта-функції.
97. Енергетичні спектри сигналів.
98. Дія детермінованих сигналів на лінійні стаціонарні системи: фізичні системи та їх математичні моделі.
99. Елементарні випромінювачі. Елементарний електричний диполь (диполь Герца).
100. Код Хаффмена. Кодове дерево.
101. Словникові методи кодування. Метод Зіва-Лемпела.
102. Матричні шифри.
103. Алгебраїчна модель шифру гамування.
104. Поточний шифр RC4.
105. Поточний шифр A5.
106. Державна, військова, комерційна і приватна конфіденційна інформація.
107. Перехоплення акустичної інформації за допомогою радіопередаючих засобів.
108. Напрямлені мікрофони. Лазерні системи контролю віконного скла.
109. Типи модуляції сигналу в охоронних системах.

110. Функції державної системи по забезпеченню інформаційної безпеки.
111. Поняття алгоритму. Лінійні, розгалужені і циклічні алгоритми.
112. Алгоритми сортування. Сортування включенням. Сортування злиттям.
113. Принцип побудови і архітектура ПК.
114. Призначення області записування та основи класифікації систем запису та відтворення інформації.
115. Оптичний запис інформації.
116. Методика магнітного запису інформації.
117. Електромагнітне поле. Система рівнянь Максвела.
118. Освітленість. Закони освітленості.
119. Збиральні та розсіювальні лінзи. Побудова зображень у лінзах.
120. Державна, військова, комерційна і приватна конфіденційна інформація. Основні визначення та поняття згідно нормативних документів. Правовий, організаційний і технічний захист інформації. Нормативні документи.
121. Загальна класифікація технічних каналів витоку інформації, яка оброблюється технічними засобами прийому, обробки, зберігання і передачі інформації (ТЗПІ).
122. Забезпечення захисту інформації від ненавмисної дії технічними засобами.
123. Класифікація візуально-оптичних та матеріально-речовинних каналів витоку інформації.
124. Способи і методи захисту інформації (ЗІ, що обробляється засобами електронної техніки, від витоку по радіотехнічному каналу).
125. Технічна реалізація пристроїв маскування.
126. Методи і засоби несанкціонованого отримання інформації по технічних каналах.
127. Методи і засоби несанкціонованого отримання інформації з автоматизованих систем (АС). Методи і засоби руйнування інформації в АС.
128. Основні методи закриття мовної інформації. Аналогові та цифрові скремблери: класифікація, принцип дії.
129. Основні підходи до створення комплексної системи запису інформації.
130. Фізичні основи оптоелектроніки. Генерація світла.
131. Джерела оптичного випромінювання.
132. Елементна база і будова оптронів.
133. Основні параметри джерел випромінювання. Основні механізми оптичного випромінювання.
134. Основні характеристики світлодіодів. Основні переваги світлодіодів, які зумовили широке застосування їх в оптоелектроніці.
135. Класифікація оптоелектронних приладів. Оптопари і оптоелектронні мікросхеми.
136. Загальна характеристика мікроелектроніки. Основні терміни і поняття, показники і фактори, що визначають сучасний розвиток мікроелектроніки. Класифікація елементної бази РЕЗ.
137. Мікроелектроніка і функціональна електроніка – основа комплексної мікромініатюризації РЕА.

138. Фізичні характеристики основних типів діодів. Пояснення особливостей їх роботи за допомогою зонних діаграм.
139. Будова, режим роботи, схеми ввімкнення біполярних транзисторів. Особливості класифікації та умовних позначень біполярних транзисторів. Фізичні параметри біполярних транзисторів. Їх режим та температурні залежності.
140. Класифікація, основні параметри будова та принцип дії тиристорів.
141. Класифікація і принцип дії польових транзисторів.
142. Основні типи ліній, шрифти, види та масштаби, які використовуються під час виконання креслення.
143. Загальні вимоги нанесення розмірів. Розмірні числа (радіус, діаметр, квадрат, нахил, конусність).
144. Проекціювання прямої. Прямі рівня та проекціюючі прямі, основні їх властивості.
145. Проекціювання площини. Площини рівня та проекціюючі площини, основні їх властивості.
146. Основні положення аксонометричного проекціювання.
147. Основні види, розрізи, перерізи та правила їх зображення на кресленнях.
148. Види типи схем, загальні вимоги їх виконання. Правила та порядок виконання структурних та принципових схем (принципова електрична схема).
149. Умовні графічні позначення радіоелектронних елементів.
150. Правила заповнення переліку елементів до схем принципових електричних.

СПИСОК ЛІТЕРАТУРИ

Основна

1. Бурячок В.Л. Інформаційна та кібербезпека: соціотехнічний аспект / В.Л. Буря чок, В. Б.Толубко, С.В. Дорошенко: К.: ДУТ, 2015 - 298 с.
2. Богуш В.М., Кудін А.М. Моніторинг і аудит систем інформаційної бе з пеки. К.: ДУІКТ, 2006, - 340 с.
3. ГСТУ СУІБ 1.0/ISO/IEC 27001:2010. Інформаційні технології. Методи захисту. Сис тема управління інформаційною безпекою. Вимоги. К.: НБУ, 2010.
4. ГСТУ СУІБ 2.0/ISO/IEC 27002:2010. Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Звід правил для управлі н ня інформаційною безпекою. К.: НБУ, 2010.
5. ДСТУ ISO/ IEC TR 13335 - 1:2003. Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 1. Концепції та моделі безпеки. К.: Держспоживстандарт України, 2005.
6. ДСТУ ISO/IEC TR 13335 - 2:2003. Інформаційні технології. Настанови з керуванн я безпекою інформаційних технологій. Частина 2. Керування та план у вання безпеки ІТ. К.: Держспоживстандарт України, 2005.
7. ДСТУ ISO/IEC TR 13335 - 3:2003. Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 3. Методи керу вання з а хистом ІТ. К.: Держспоживстандарт України, 2005.
8. ДСТУ ISO/IEC TR 13335 - 4:2005. Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 4. Настанови з керування безпекою інформаційних технологій. К.: Держспоживстанд арт України, 2005.
9. ДСТУ ISO/IEC TR 13335 - 5:2005. Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 5. Настанови з керування мережною безпекою. К.: Держспоживстандарт України, 2005.
10. Конституція України / Верховна Рада України. – Офіц. вид. – К.: Відомості Верховної Ради України, 1996. – No 30. – Ст. 141.
11. Про інформацію [Електронний ресурс] Закон У країни від 02.10.2002 р. No 2657 - XII. – Режим доступу: http.rada.gov.ua. – Заголовок з екрану. 9
12. Про державну таємницю [Електронний ресурс] Закон України від 21.09.1999 р. No 1079 - XIV. – Режим доступу: http.rada.gov.ua. – Заголовок з екрану.
13. Про захист інформації в інформаційно - телекомунікаційних системах [Електронний ресурс] Закон України від 05.10.1994 р. No 80/94 - ВР. – Режим доступу: http.rada.gov.ua. – Заголовок з екрану.
14. Про надзвичайний стан [Електронний ресурс] Закон України від 26.06.1992 р. No 2501 - XI I. – Режим доступу: http.rada.gov.ua. – Заголовок з екрану.
15. Кримінальний кодекс України [Електронний ресурс] Закон України від 05.04.2001 р. No 2341 - III. – Режим доступу: http.rada.gov.ua. – Заголовок з екрану.

16. Цивільний процесуальний кодекс України [Електр онний ресурс] Закон України від 18.03.2004 р. No 1618 - IV. – Режим доступу: http.rada.gov.ua. – Заголовок з екрану.
17. Базові поняття. Терміни та визначення : ДСТУ 2392 - 94. – [Чинний від 01 – 01 – 1995]. – К. : Держстандарт України, 1994. – IV. 89 с. – (Держав ний стандарт України).
18. Технічний захист інформації. Основні положення : ДСТУ 3396.0 - 96. – [Чинний від 1997 – 01 – 01]. – К.: Держстандарт України, 1995. – IV. 8 с. (Державний стандарт України).
19. Технічний захист інформації. Порядок проведення робіт : ДС ТУ 3396.1 - 96. – [Чинний від 1997 – 01 – 07]. – К.: Держстандарт України, 1995. – IV. 11 с. (Державний стандарт України).
20. Технічний захист інформації. Терміни та визначення : ДСТУ 3396.2 - 97 – [Чинний від 1998 – 01 – 01]. – К.: Держстандарт України, 1995 . – IV. 12 с. (Державний стандарт України).
21. Процеси життєвого циклу програмного забезпечення (ISO/IEC 12207: 1995) : ДСТУ 3918 - 1999 – [Чинний від 2000 - 07 - 01]. – К. : Держстандарт України, 2000. VI. 49 с. (Державний стандарт України).
22. Настанови з керуванн я безпекою інформаційних технологій. Частина 1. Концепції та моделі безпеки інформаційних технологій : ДСТУ ISO/IEC TR 13335 - 1:2003. – [Чинний від 2004 – 10 – 01]. – К. : Держспоживстандарт України, 2005. – IV. 17 с. – (Національний стандарт України).
23. Настанови з керування безпекою інформаційних технологій. Частина 2. Керування та планування безпеки інформаційних технологій : ДСТУ ISO/IEC TR 13335 - 2:2003. – [Чинний від 2004 – 10 – 01]. – К. : Держспоживстандарт України, 2005. – IV. 16 с. – (Національний ста ндарт України).
24. Настанови з керування безпекою інформаційних технологій. Частина 3. Методи керування захистом інформаційних технологій : ДСТУ ISO/IEC TR 13335 - 3:2003. – [Чинний від 2004 – 10 – 01]. – К. : Держспоживстандарт України, 2005. – V. 42 с. – (Н аціональний стандарт України).
25. Настанови з керування безпекою інформаційних технологій. Частина 4. Вибір засобів захисту : ДСТУ ISO/IEC TR 13335 - 4:2005. – [Чинний від 2006 – 07 – 01]. – К. : Держспоживстандарт України, 2007. – XI. 56 с. – (Національний стандарт України).
26. Настанови з керування безпекою інформаційних технологій. Частина 5. Настанова з керування мережною безпекою: ДСТУ ISO/IEC TR 13335 - 5:2005. – 10 [Чинний від 2006 – 07 – 01]. – К. : Держспоживстандарт України, 2007. – VII. 23 с. – (Національ ний стандарт України).
27. Нормативне забезпечення інформаційної безпеки / [Головань С. М., Петров О. С., Хорошко В. О. та ін.]. – К. : Державний університет інформаційно - комунікаційних технологій, 2008. – 533 с.
28. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу : НД ТЗІ 1.1 - 002 - 99. – Офіц. вид. – К. : НікС : Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, 1999. – III. 15 с. (Нормативний документ системи технічно го захисту інформації).

29. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу : НД ТЗІ 1.1. - 003 - 99. – Офіц. вид. – К. : НікС : Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, 1999. – ІІІ. 24 с. (Нормативний документ системи технічного захисту інформації).
30. Типове положення про службу захисту інформації в автоматизованій системі : НД ТЗІ 1.4 - 001 - 2000. – Офіц. вид. – К. : НікС : Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, 1999. – ІІІ. 20 с. (Нормативний документ системи технічного захисту інформації).
31. Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах к ласу 2 : НД ТЗІ 2.5 - 008 - 2002. – Офіц. вид. – К. : НікС : Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, 2002. – ІІІ. 25с. (Нормативний документ системи технічного захисту інформації).
32. Головань С. М. Вимоги до побудови моделі загроз інформаційних систем / С. М. Головань // Інформаційна безпека – 2009. – No 2 (2) – С. 77 – 84.
33. Класифікація інформації / С. М. Головань, А. М. Давиденко, Л. М. Щербак [та ін] // Защита информации: Сб. науч. тр. Национального авиационного университета. – 2005. – Вып. 12. – С. 8 – 16.
34. Несанкціоноване використання інформації та відповідальність за ці дії / С. М. Головань, А. М. Давиденко, О. О. Мелешко [та ін.] // Моделювання та інформаційні технології. Зб. наук. праць Інституту проблем моделювання в енергетиці ім. Г. Є. Пухов а НАН України. – 2005. – Вип. 35. – С. 3 – 7.
35. Ленков С.В., Перегудов Д.А. Хорошко В.А. Методы и средства защиты информации. Том 1. Несанкционированное получение информации. К.: Изд а тельство Арий, 2008.
36. Ленков С.В., Перегудов Д.А. Хорошко В.А. Методы и средст ва защиты информации. Том 2. Информационная безопасность. К.: Издательство Арий, 2008.
37. Хорошко В.А., Чекатков А.А. Методы и средства защиты информации. К.: Изд. Юниор, 2003. – 504с.
38. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Електронний підручник. Харків, ХНУРЕ, 2011 р.
39. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Електронний конспект лекцій. Харків, ХНУРЕ, 2011 р.
40. Горбенко І. Д. Гриненко Т. О. Захист інформації в інформаційно-телекомунікаційних системах: Навч. посібник. Ч.1. Криптографічний захист інформації - Харків: ХНУРЕ, 2004 - 368 с.
41. Горбенко Ю.І., Горбенко І.Д. Інфраструктури відкритих ключів . Системи ЕЦП. Теорія та практика. Харків. Форт. 2010 , 593с.
42. Есин В. И., Кузнецов А. А., Сорока Л. С. Безопасность информационных систем и технологий – Х.:ООО «ЭДЭНА», 2010.-656с.

Додаткова

1. Васильєва Л.Д.. Напівпровідникові прилади : підруч. / Л.Д. Васильєва, Б.І. Медведенко, Ю.І .Якименко. – К. : Політехніка, 2003.
2. Воробієнко П.П., Нікітюк Л.А., Резніченко П.І. Телекомунікаційні та інформаційні мережі. – К.: Самміт-книга, 2010
3. Автоматические системы коммутации: Учебник для вузов/ под ред. Иванова О.Н., Копп М.Ф., Коханова З.С…. – М.: Связь, 1978. -624 с.
4. Интегральная оптика./ Под ред. Т.Тамира.- М.: Мир, 1978.- 344 с.
5. Задірака В. Компьютерна криптологія. Підручник. К, 2002 ,504с.
6. В. Столлингс. Криптография и защита сетей. Принципы и практика. Изд. “Вильямс”.К. 2001. 669 с.
7. Бессалов А., Телиженко А. Криптосистемы на эллиптических кривых. – К.: «Політехніка», 2004. – 224 с.
8. Радіотехніка № 114, 119, 126, 134, 141, 142,145.Всеукраїнський міжвідомчий збірник.Харків, ХНУРЕ, 2000- 2008 рр.
9. Прикладная радиоелектроника. Научн. техн. журнал. Академія наук прикладної радіоелектроніки, ХНУРЕ. Тематические выпуски «Безопасность информации» №2- 2006; №2, №3-2007, №3- 2008, №3 – 2009, № 3 – 2010, №2 – 2011рр.

Критерії оцінювання результатів вступного фахового іспиту (тестування)

Тест складається з 20 завдань. За кожну правильну відповідь нараховується 6 балів. Загальна оцінка за тест дорівнює сумі набраних балів, збільшеній на 80 балів. Отриманий результат знаходиться в межах від 80 до 200 балів. Для допуску до участі в конкурсі на фаховому вступному випробуванні потрібно отримати не менше 100 балів.