Затверджую
Голова приймальної комісії
НУ «Запорізька політехніка»
_____ проф. Віктор ГРЕШТА
« 12 » травня 2022 року

ПРОГРАМА

фахового іспиту для абітурієнтів, які вступають до НУ «Запорізька політехніка» на навчання за освітнім ступенем «магістр» на основі раніш здобутого освітнього ступеня «бакалавр», «магістр» або освітньо-кваліфікаційного рівня «спеціаліст» за спеціальністю *125 «Кібербезпека»*.

Для оцінки знань абітурієнтів на фаховому іспиті фаховою атестаційною комісією розроблені критеріально-орієнтовані тестові завдання, які дозволяють встановити рівень сформованості компетентностей необхідних для засвоєння змісту навчання за спеціальністю *125 «Кібербезпека»* ступеня «магістр».

Фаховий іспит може проводитись очно та/або дистанційно із використанням інформаційного сервісу «Система дистанційного навчання» НУ «Запорізька політехніка». При проведенні в дистанційному форматі обов'язковою є процедура візуальної ідентифікації вступника, здійснюється відеофіксація іспиту.

Вступники повинні знати і вміти:

- теоретичні основи моделювання, аналізу та синтезу електричних кіл, сигналів та процесів в інформаційних і телекомунікаційних системах;
- основні поняття теорії інформації, інформаційних процесів і кодування, існуючі підходи та алгоритми для розв'язання проблем завадостійкого і ефективного кодування, компресії, передачі і зберігання інформації;
- виявляти та усувати шкідливі програми (комп'ютерні віруси) з використанням сучасних антивірусних програм;
- загальні принципи побудови та функціонування інтелектуальних систем;
- методи створення алгоритмів та програм, мову програмування С, та її розширення С++, основні типи даних, розробляти алгоритм вирішення задачі згідно технічного завдання; розробляти код на мові програмування С++; проводити тестування програмних модулів; визначати ефективність алгоритмів та програм;
- основні поняття, функції, склад та принципи роботи операційних систем, характеристики моделей баз даних, конструкції мов опису та маніпулювання даними, класифікацію систем передачі інформації; характеристики сигналів електрозв'язку, алгоритми кодування лінійних сигналів, методи доступу проводових і рухомих стандартів зв'язку,

вирішувати задачі адміністрування операційних систем і баз даних, моделювати предметні області та проектувати бази даних, оцінювати основні методи передачі повідомлень, обгрунтовувати вибір методу розділення каналів;

- призначення різних протоколів стеку TCP\IP; класифікацію мереж, призначати IP-адреси, розраховувати параметри підмереж;

- методи аналізу загроз, фізику виникнення каналів витоку інформації, демаскуючі признаки каналів витоку інформації, принципи побудови і структури захищених інформаційно-комунікаційних систем, активні та пасивні методи захисту інформації, основи спеціальних вимірювань параметрів систем безпеки;

- структуру каналу зв'язку, принципи дії функціональних блоків таких каналів;

- загальні криптоперетворення, криптографічні стандарти, застосовувати стандартні криптографічні алгоритми та протоколи для захисту інформації;

- класифікацію загроз безпеці інформаційних ресурсів; основні положення методів та способів правового, організаційного та інженерно-технічного захисту інформації; існуючі системи безпеки банку та їх функції, методи забезпечення безпеки електронних платіжних системи, аналізувати моделі загроз інформаційним ресурсам, оцінювати можливі ризики інформаційної безпеки, використовуючи сучасні програмні комплекси.

При підготовці завдань комісія виділила такі основні розділи з переліком тем:

1. Основи теорії кіл, сигналів і процесів в електроніці:

- Основні поняття і закони електричних кіл.
- Аналіз лінійних кіл постійного струму.
- Аналіз часових та частотних характеристик лінійних кіл.
- Основи теорії чотириполюсників.
- Спектральний та операторній аналіз сигналів і лінійних кіл.
- Дискретні сигнали та цифрові фільтри.
- Аналіз нелінійних кіл та нелінійних перетворень сигналу.

2. Інформаційна безпека:

- Основні поняття теорії інформації, інформаційних процесів.
- Завадостійке і ефективне кодування, компресія, передача і зберігання інформації.
- Загрози безпеці комп'ютерних систем та міри протидії.
- Принципи побудови, класифікація та особливості комп'ютерних вірусів.
- Основні поняття штучного інтелекту.
- Розпізнавання образів.

3. Технології програмування:

- Основні елементи синтаксису мови програмування C++ та типи даних.

- Базові конструкції структурного програмування: процес, розгалуження, цикл.
- Динамічний розподіл пам'яті, операції з покажчиками, динамічні структури даних.
- Модульне програмування. Фактичні та формальні параметри.
- Передача параметрів за значенням, за покажчиком та за посиланням.
- Обробка строкових даних.
- Основи об'єктно-орієнтованого програмування.

4. Захищені операційні системи та бази даних. Системи передачі інформації:

- Класифікація програмного забезпечення.
- Типи, складові та функції операційних систем.
- Локальні і розподілені бази даних.
- Характеристики сигналів електрозв'язку.
- Параметри каналів цифрових систем передачі інформації.
- Характеристики ієрархій та стандартів передачі інформації.

5. Мережеві технології, системи комутації і протоколи:

- Стек протоколів TCP\IP.
- Призначення IP-адрес.
- Класифікація мереж.
- Визначення маски підмережі.

6. Системи технічного захисту інформації:

- Фізико-технічні методи захисту інформації.
- Методи та засоби захисту інформації в інформаційно-комунікаційних системах.
- Спеціальні вимірювання в системах захисту інформації.

7. Пристрої передачі, прийому та обробки інформації:

- Узагальнена структурна схема каналу зв'язку.
- Дротовий і радіоканал. Порівняльний аналіз галузі застосування.
- Призначення і вимоги до кожного елемента структурної схеми каналу зв'язку.

8. Прикладна криптографія:

- Симетричні криптосистеми.
- Асиметричні криптосистеми.
- Стандарти шифрування.
- Стандарти цифрового підпису.

9. Менеджмент і організаційне забезпечення інформаційної безпеки. Безпека комерційної діяльності:

- Стандарти управління інформаційною безпекою.
- Програмні комплекси оцінки ризиків інформаційної безпеки.
- Системи банківської безпеки.
- Безпека електронної комерції.
- Організаційно-правові методи захисту інформації.

КРИТЕРІЇ ОЦІНЮВАННЯ

Оцінювання здійснюється за 100 бальною шкалою від 100 до 200 балів або ухвалюється рішення про негативну оцінку вступника («незадовільно»).

Кожний варіант тестів містить 30 завдань, які розподілені за трьома рівнями складності (по 10 завдань кожного рівня). Складність екзаменаційних завдань визначається, як правило, кількістю логічних кроків, які повинен виконати абітурієнт у процесі пошуку відповіді.

1-й рівень містить 10 завдань мінімального рівня складності, для відповіді на які достатньо орієнтуватися в основних поняттях щодо інформаційної безпеки.

Правильна відповідь на кожне завдання цього рівня оцінюється двома балами.

Оскільки актуальним напрямом кібербезпеки є конкретні технології захисту інформації, то 2-й рівень, який містить 10 завдань середнього рівня складності, дозволяє з'ясувати рівень знань абітурієнта щодо властивостей алгоритмів захисту.

Правильна відповідь на кожне завдання цього рівня оцінюється трьома балами.

3-й рівень містить 10 завдань підвищеної складності, відповідь на які вимагає володіння абітурієнтом практичним використанням методів кібербезпеки.

Правильна відповідь на кожне завдання цього рівня оцінюється п'ятьма балами.

Отже, максимальна кількість балів, яку абітурієнт може отримати за правильно виконані завдання всіх трьох рівнів, складає 200 балів.

Вступник допускається до участі у конкурсному відборі для зарахування на навчання, якщо кількість отриманих балів становить більше ніж 100 балів.

У разі наявності в паперовій роботі більше однієї відміченої відповіді на кожне запитання, за це запитання виставляється нуль балів (окрім випадків, коли одна з відмічених відповідей на запитання закреслена, а інша зазначена акуратно та чітко).

Усі попередні кроки і міркування, що приводять до відповіді на завдання, абітурієнт виконує на чернетці. Перевірка цих записів екзаменаторами не передбачається. Екзаменатори перевіряють лише вірність закреслених відповідей серед запропонованих на кожне завдання варіантів А, Б, В, Г, Д, Е в листі відповіді.

СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

1. Основи теорії кіл, сигналів та процесів в системах технічного захисту інформації: підручник для студентів вищих навчальних закладів. Ч.1 / Ю.О. Коваль, І.О. Милютченко, А.М. Олейніков, В.М. Шокало та ін; за заг. редакцією В.М. Шокала. – Харків: НТМТ, 2011. – 544 с.

2. Соболев Ю.В., Бабаев М.М., Давиденко М.Г. Теорія електричних і магнітних кіл. – Харків: ХФВ «Транспорт України», 2002. – 264 с.

3. Бессонов Л.А.Теоретические основы электротехники. Электрические цепи: Учеб. Для вузов. Изд. 10-е. - М.: Гардарики, 2002. - 638 с.

4. Попов В.П. Основы теории цепей: Учеб. для вузов. Изд. 3-е - М.: Высшая школа, 2000. - 575с.

5. Захист інформації в комп'ютерних системах та мережах : навч. посіб. / С.Г.Семенов, А.О.Подорожняк, О.І.Баленко, С.Ю.Гавриленко – Х.: НТУ «ХПІ», 2014.– 251с.

6. Інтелектуальні системи : навч. посіб. / С. О. Субботін, А. О. Олійник ; за ред. С. О. Субботіна. - Запоріжжя : ЗНТУ, 2014. - 219 с.

7. Жураковський Ю. П. Теорія інформації та кодування: [Підручник] / Ю. П. Жураковський, В. П. Полторак. – К. : Вища школа, 2001.– 255 с.

8. Прата С. Язык программирования C++. Лекции и упражнения. – Киев : Издательство : Диалектика-Вильямс, 2020. — 1248 с.

9. Шилдт Г. C++ : базовый курс. – Киев : Диалектика, 2019. – 624 с.

10. Шилдт Г. Самоучитель C++: Пер. с англ. — 3-е изд. — СПб.: БХВ-Петербург, 2003. — 688 с.

11. Павловская Т.А. C/C++. Программирование на языке высокого уровня. - СПб.: Питер, 2003.- 461 с.

12. Макконел Дж. Основы современных алгоритмов. М. : Техносфера, 2006. – 368 с.

13. Федотова-Півень І.М. Операційні системи : навч. посібник / І.М. Федотова-Півень, І.В. Миронець, О.Б. Півень, С.В. Сисоєнко, Т.В. Миронюк. –Харків : ТОВ «ДІСА ПЛЮС», 2019. –216 с.

14. Трофименко О.Г. Організація баз даних: навч. посібник / О.Г. Трофименко, Ю.В. Прокоп, Н.І. Логінова, І.М. Копитчук. – Одеса: Фенікс, 2019. – 246с.

15. Браїловський В.В. Багатоканальні системи передачі інформації: навч. посібник / В.В. Браїловський, М.Г. Рождественська. – Чернівці: ЧНУ, 2017. – 140 с.

16. Кунегин, С.В. Системы передачи информации / С.В. Кунегин. – М.: в/ч 33965, 1997. – 317с.

17. Крэйг Хант TCP/IP. Сетевое администрирование, 3-е издание. - Пер. с англ. - СПб: Символ-Плюс, 2007. - 816 с.

18. Microsoft TCP/IP. Учебный курс: Официальное пособие Microsoft для самостоятельной подготовки: Пер. с англ. — 3-е изд., испр. — М.: Русская редакция, 2001. — 400 с.

19. Ногл М. TCP/IP. Иллюстрированный учебник — М.:ДМК Пресс, 2001. — 480 с.

20. Бузов Г.А. Защита от утечки информации по техническим каналам: Учебное пособие. / Г.А. Бузов, С.В. Калинин, А.В. Кондратьев А.В. / М.: Горячая линия – Телеком, 2005. – 416 с.

21. Хорошко В.А. Методы и средства защиты информации. / В.А. Хорошко, А.А. Чекатков, под ред. Ю.С.Ковтанюка. – К.: Издательство Юниор, 2003. – 504 с.

22. Архипов О.Є. Захист інформації в телекомунікаційних мережах та системах зв'язку: Навч.-метод. посіб. / Архипов О.Є., Луценко В.М., Худяков В.О. – Київ: Політехніка, 2003. – 400с.

23. Архипов О.Є. Застосування методології передбачення для оцінювання шкоди, заподіяної витоком секретної інформації [Текст] / О.Є.Архипов, І.П. Касперський //

Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні. – Вип.2(15). – К.: 2007. – С.13-19.

24. Шишкин Г. Г., Шишкин А. Г. Электроника: учебник для вузов. Режим доступу: http://www.vipbook.su/tehnika/elektronika/187566-elektronika-uchebnik-dlya-vuzov.html.

25. Зорі, А.А. Аналогова схемотехніка та імпульсні пристрої [Електронний ресурс]: електронний підручник /А.А. Зорі, В.П. Тарасюк, О.М. Стародубцева, О.В. Вовна. ДонНТУ. – Донецьк, 2008. – 1 електрон. опт. диск (DVD-ROM); 12 см. – Режим доступу: http://fkita.donntu.edu.ua/et/book/obobshen/index.html. – Загл. з екрану. (Гриф МОНУ № 14/18-Г-1656 від 7.07.2008 р.).

26. Горбенко І.Д. Прикладна криптологія / Горбенко І.Д., Горбенко Ю.І. – Харків: Видавництво «Форт», 2012. – 878 с.

27. Конахович Г.Ф. Компьютерная стеганография. Теория и практика / Конахович Г.Ф., Пузыренко А.Ю. – К.: МК-Пресс, 2006. – 288 с.

28. Козіна Г.Л. Криптографія від історії до сучасних стандартів: навч.посібник/ Г.Л. Козіна. – Запоріжжя: НУ «Запорізька політехніка», 2020. – 192 с. – http://eir.zntu.edu.ua/handle/123456789/6528

29. Пістунов І.М. Безпека електронної комерції: навч. посібник / І.М. Пістунов, Є.В. Кочура. – Д.: НГУ, 2014. – 125 с.

30. Тардаскіна Т.М. Менеджмент інформаційної безпеки в галузі зв'язку: навч. посібник / Т.М. Тардаскіна, В.Г Кононович. – Одеса: ОНАЗ, – 2010. – 268 с.

31. Корченко О.Г. Аудит та управління інцидентами інформаційної безпеки: навч. посібник / О.Г. Корченко, С.О. Гнатюк, С.В. Казмірчук. – К.: Центр навч.-наук. та наук.-пр. видань НА СБ України, 2014. – 190с.

32. Карпуков Л. М. Основи теорії кіл, сигналів та процесів в електроніці: навчальний посібник для студентів вищих навчальних закладів/ Ч.1. / Л. М. Карпуков – Запоріжжя: НУ «Запорізька політехніка», 2021. – 163 с.

Затверджено на засіданні
фахової атестаційної комісії
спеціальності *125 «Кібербезпека»*
«_12_» _травня_ 2022р.

Голова фахової атестаційної комісії
спеціальності *125 «Кібербезпека»* Галина КОЗІНА