Затверджую
Голова приймальної комісії ЗНТУ

проф. Бєліков С.Б.
« 10 » березня 2017 року

ПРОГРАМА

вступного екзамену з фаху для абітурієнтів, які вступають до ЗНТУ на навчання за освітнім ступенем «магістр» на базі раніш здобутого освітнього ступеня «бакалавр» або освітньо-кваліфікаційного рівня «спеціаліст».

Для оцінки знань абітурієнтів з вступного екзамену фаховою атестаційною комісією розроблені критеріально-орієнтовані тестові завдання, які дозволяють встановити рівень сформованості компетенцій необхідних для засвоєння змісту навчання за спеціальністю 125 «Кібербезпека» («Системи технічного захисту інформації, автоматизація її обробки») ступеня «магістр».

Вступники повинні знати і вміти:

– основи програмування, інформатики й сучасних інформаційних технологій;

– нормативно-правову базу й політику безпеки в галузі захисту інформації, менеджмент інформаційної безпеки та сучасні стандарти безпеки інформаційних технологій;

– методи аналізу загроз і каналів витоку інформації, принципи побудови і структури систем технічного захисту інформації;

– основи електроніки, принципи функціонування пристроїв обробки, передавання та захисту інформації;

– теоретичні основи передавання інформації, принципи і методи обробки, кодування і стиснення інформації;

– основи загальної і прикладної криптографії, сучасних стандартів криптографічних систем захисту інформації;

– мережеві технології, системи комутації, протоколи та стандарти;

– програмно-апаратні засоби ідентифікації та автентифікації, методи захисту операційних систем та баз даних, сучасні уявлення про методи захисту в банківських технологіях та економічній діяльності;

– використовувати професійно-профільовані знання й практичні навички з виявлення й блокування каналів несанкціонованого доступу до інформації, джерел і способів дестабілізуючого впливу на інформацію;

– створювати моделі загроз і об'єктів захисту з використанням нормативних документів, методів математичного моделювання та необхідних видів, методів, засобів і технологій захисту інформації;

– проводити аудит інформаційної безпеки, сертифікацію та експертні дослідження систем, засобів та технологій захисту інформації.

При підготовці завдань комісія виділила такі основні дисципліни:
1. Інформаційні технології
2. Правові основи охорони інформації
3. Основи теорії кіл, сигналів та процесів в системах технічного захисту інформації
4. Теорія інформації та кодування
5. Мережеві технології, системи комутації та протоколи
6. Системи передачі інформації
7. Захищені операційні системи та бази даних
8. Методи та засоби технічного захисту інформації
9. Управління інформаційною безпекою
10. Засоби приймання та обробки інформації в системах технічного захисту інформації
11. Криптографія та стеганографія
12. Технічні засоби охорони об'єктів

КРИТЕРІЇ ОЦІНЮВАННЯ

Оцінювання здійснюється за 100 бальною шкалою від 0 до 100 балів.

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 та визначеннях.

Правильна відповідь на кожне завдання цього рівня оцінюється двома балами.

2-й рівень містить 10 завдань середнього рівня складності, для відповіді на які необхідно мати базові знання та оперувати ними.

Правильна відповідь на кожне завдання цього рівня оцінюється трьома балами.

3-й рівень містить 10 завдань підвищеної складності, відповідь на які дозволяє виявити рівень загально-наукової та професійної компетенції.

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 100 балів.

Вступник допускається до участі у конкурсному відборі для зарахування на навчання, якщо кількість отриманих балів становить не менше 2.

У разі наявності в 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: підручник для студентів вищих навчальних закладів. Ч1 / Ю.О. Коваль, Л.В. Гринченко, І.О.Милютченко, О.І. Рибін / За заг. редакцією В.М.Шокало, В.І. Правди. – Х.: Компанія СМІТ, 2008. – 432 с.
2. Основи теорії кіл: підручник для студентів вищих навчальних закладів. Ч2 / Ю.О. Коваль, Л.В. Гринченко, І.О.Милютченко, О.І. Рибін / За заг. редакцією В.М.Шокало, В.І. Правди. – Х.: Компанія СМІТ, 2008. – 560 с.
3. Волощук Ю.І. Сигнали та процеси у радіотехніці: Підручник для студентів вищих навчальних закладів – Харків: Компанія СМІТ, 2003. – т.1 -580 с., т. 2 - 444 с.
4. Основы теории передачи информации. Ч1.Экономное кодирование / В.И. Шульгин. – Учеб. пособие. – Харьков: Нац. аэрокосм. ун-т «Харьк. авиац. ин-т», 2003. – 102 с.
5. Основы теории передачи информации. Ч2. Помехоустойчивое кодирование / В.И. Шульгин. – Учеб. пособие. – Харьков: Нац. аэрокосм. ун-т «Харьк. авиац. ин-т», 2003.– 87с.
6. 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. – 40с.
7. 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.
8. 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.Слепцов В.І. Правове та нормативне забезпечення інформаційної безпеки. Монографія – Запоріжжя: Вид-во ЗНТУ, 2010. – 152с.
9. Цимбалюк В.С., Гавловський В.Д., Гриценко В.В. та ін. Основи інформаційного права України.: Навч. посіб./О-72. – К.: Знання, 2004. – 274 с.
10. 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.
11. Архипов А.К. Применение среднего риска для оценивания эффективности защиты информационных систем [Текст] / А.Е. Архипов // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – Вип.1(14). – К.: 2007. – С.60-67.
12. HASP 4. Руководство программиста.
13. Горбенко Ю.І. Інфроструктури відкритих ключів. Електронний цифровий підпис. Теорія та практика: монографія. [текст] / Горбенко Ю.І., Горбенко І.Д. – Харків: Видавництво «Форт», 2012. – 608 с.
14. Касперский Е.В. Компьютерное зловредство. – СПб.: Питер, 2009. – 208 с.
15. Бузов Г.А., Калинин С.В., Кондратьев А.В. Защита от утечки информации по техническим каналам: Учебное пособие.-М.:Горячая линия-Телеком, 2005.-416с.
16. Цифровые и аналоговые системы передачи: Учебник для вузов / В.И.Иванов, В.Н.Гордиенко, Г.Н.Попов и др.; Под ред. В.И.Иванова. – 2е изд. – М.: Горячая линия – Телеком, 2003. – 232 с.

17. Защита информации в системах мобильной связи: Учебное пособие для вузов / А.А. Чекалин, А.В. Заряев, С.В. Скрыль и др.; под ред. А.В. Заряева, С.В. Скрыля – 2-е изд. испр. и доп. – М.: Горячая линия – Телеком, 2005. – 171 с.

18. Построение коммутируемых компьютерных сетей: учебное пособие / Е.В. Смирнова и др. — М.: Национальный Открытый Университет «ИНТУИТ»: БИНОМ. Лаборатория знаний, 2011. — 367 с.

19. А. Ретана, Д. Слайс, Т. Уайт. Принципы проектирования корпоративных IP-сетей – М.: Вильямс, 2002 – 367с.

20. Е.В. Смирнова, А.В. Пролетарский, И.В. Баскаков, Р.А. Федотов. Управление коммутируемой средой – М.: РУСАКИ, 2011 – 335с.

21. Електродинаміка та поширення радіохвиль: в 2т. / В.М. Шокало, В.І. Правда, В.А. Усін та ін. – Харків: Колегіум, 2010.

22. Бармен Скотт. Разработка правил информационной безопасности. М.: Вильямс, 2002. — 208 с.

23. Запечников С. В., Милославская Н. Г., Толстой А. И., Ушаков Д. В. Информационная безопасность открытых систем. В 2-х тт.:Том 1. Угрозы, уязвимости, атаки и подходы к защите. М.: Горячая Линия — Телеком, 2006. — 536 с. Том 2. Средства защиты в сетях. М.: Горячая Линия — Телеком, 2008. — 560 с.

24. Оппенгейм А. Цифровая обработка сигналов / А. Оппенгейм, Р.Шафер. – М.: Техносфера, 2006. – 856с.

25. Айфичер Э. Цифровая обработка сигналов: практический подход / Э.Айфичер, Б. Джервис; 2-е изд.: Пер. с англ. – М.: Издательский дом «Вильямс», 2004. – 992 с.

26. А.В.Галицкий, С.Д.Рябко, В.Ф. Шаньгин. Защита информации в сети – анализ технологий и синтез решений. М.: ДМК Пресс, 2004. – 616 с.

27. В.В.Домарев. Безопасность информационных технологий. Системный подход. К.: ООО «ТИД «ДС», 2004. – 992 с.

Затверджено на засіданні фахової атестаційної комісії спеціальності 125 «Кібербезпека» («Системи технічного захисту інформації, автоматизація її обробки»)
01 березня 2017 року

Голова фахової атестаційної комісії
спеціальності 125 «Кібербезпека»
(«Системи технічного захисту інформації,
автоматизація її обробки») С.І. Лізунов