МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВІННИЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖЕНО
Вченою радою ВНТУ
протокол № 5
від «19» грудня 2017 р.
проректор з наукової роботи
_____ С. В. Павлов

ПРОГРАМА
вступного іспиту до аспірантури за спеціальністю
125 – кібербезпека
галузь знань 12 – Інформаційні технології

Розглянуто і схвалено
Секцією Науково-технічної ради
ВНТУ
протокол № 1
від «25» жовтня 2017 р.
голова секції НТР
_____ О. В. Грушко

Вінниця 2017

1. «Основи інформаційної безпеки»

1. Поняття інформаційної безпеки, системи захисту інформації. Функції та вимоги до систем захисту інформації. Концептуальна модель інформаційної безпеки.
2. Напрямки та засоби захисту інформації.
3.Загрози конфіденційності інформації.
4. Способи доступу до конфіденційної інформації.
5. Характеристика правового захисту інформації. Структура правових актів, що орієнтовані на правовий захист. Спеціальне законодавство в галузі інформаційної безпеки.
6. Характеристика організаційного захисту інформації. Основні організаційні заходи інформаційної безпеки. Служба безпеки підприємства.
7. Характеристика технічного захисту інформації.
8. Фізичні засоби захисту інформації. Охоронні системи. Системи контролю доступу.
9. Апаратні та програмні засоби захисту інформації.
10. Політика інформаційної безпеки. Основні сервіси безпеки.
11. Інформаційно-психологічна безпека людини, суспільства та держави. Психологічна війна.

2. «Криптографія та стеганографія».

1. Задачі криптографії. Модель криптографічної системи. Класифікація криптографічних систем. Вимоги до шифрів.
2. Основні поняття про стійкість шифрів. Підходи до оцінювання стійкості.
3. Застосування, переваги та недоліки симетричного шифрування.
4. Потокове шифрування.
5. Генератори псевдовипадкових послідовностей.
6. Аналіз статистичної безпеки криптоалгоритмів. Методики оцінювання якості генераторів ПВП.
7. Симетричне блокове шифрування.
8. Розподіл секретних ключів відкритим каналом зв’язку.
9. Асиметричне шифрування інформації.
10. Автентифікація сторін взаємодії.
11. Цифрове підписування.
12. Криптографічні хеш-функції.
13. Криптографічні алгоритми та протоколи.
14. Арифметика виконання операцій над числами великої розрядності. Вирішення проблем вибору параметрів криптографічних алгоритмів
15. Стеганографічний захист інформації. Прихована інформація. Контейнер.
16. Математична модель стеганосистем. Стеганографічні протоколи.
17. Основні властивості зорової системи людини, що використовуються при приховуванні даних в зображеннях.
18. Приховування даних у просторовій області зображень. Методи приховування в найменш значущому біті даних.

19. Приховування даних у просторовій області зображень із застосуванням складних дискретних сигналів.

3. «Комплексні системи захисту інформації».

1. Історичні аспекти формування поняття систем захисту інформації.
2. Класифікація автоматизованих систем. Профілі захисту інформації. Визначення області та межі дії КСЗІ.
3. Організаційні та інженерно-технічні заходи безпеки.
4. Об’єкти інформаційних відносин. Суб’єкти інформаційних відносин, основні права й обов’язки учасників зазначених відносин.
5. Нормативно-правове забезпечення КСЗІ.
6. Методи та засоби інженерно-технічних заходів безпеки.
7. Структура КСЗІ. Обґрунтування створення КСЗІ.
8. Етапи побудови КСЗІ. Ресурси як основні об'єкти КСЗІ.
9. Методика впровадження КСЗІ.
10. Оцінювання рівня загроз та вразливостей.
11. Системний підхід в управлінні КСЗІ.
12. Вимоги до проведення випробувань КСЗІ. Програма, тривалість і область діяльності випробувань КСЗІ.
13. Атестація, сертифікація, експертиза та супроводження КСЗІ.

4. «Системи менеджменту інформаційної безпеки».

1. Історичні аспекти формування поняття системи менеджменту.
2. Визначення області та межі дії систем менеджменту інформаційної безпеки.
3. Структура систем менеджменту.
4. Місце і роль системи менеджменту інформаційної безпеки в управлінні діяльністю організацій.
5. Людина та соціальна група як суб’єкт інформаційної безпеки. Роль та місце таких суб’єктів в захисту інформації з обмеженим доступом.
6. Критерії оцінки інформаційної безпеки за національними стандартами.
7. Критерії оцінки інформаційної безпеки міжнародними стандартами.
8. Міжнародний стандарт ISO / IEC 15408.
9. Структура та вимоги стандарту ISO/IEC 27001.
10. Структура стандарту ISO/IEC 27002.
11. Система управління ризиками на вимогу стандарту ISO/IEC 27001:2005.
12. Методики впровадження системи менеджменту інформаційної безпеки.
13. Принципи QECD.
14. Модель PDCA.
15. Технології оцінки інформаційних ризиків.
16. Технології аналізу інформаційних ризиків.
17. Інтеграція системи менеджменту інформаційної безпеки за вимогами ISO/IEC
18. Вимоги стандарту ISO 19011:2002 до проведення аудитів.
19. Аудит систем менеджменту інформаційної безпеки.

20. Види аудиту.
21. Етапи внутрішнього аудиту систем менеджменту інформаційної безпеки.

5. Конкурентна розвідка.

1. Історія становлення та розвитку конкурентної розвідки
2. Поняття конкурентної розвідки
3. Завдання та особливості конкурентної розвідки
4. Організація роботи підрозділу конкурентної розвідки
5. Напрями діяльності конкурентної розвідки
6. Класифікація джерел для інформаційної бази даних конкурентної розвідки
7. Стратегія та шляхи визначення інформаційних потреб керівництва компанії в діяльності конкурентної розвідки
8. Методика конкурентної розвідки
9. Протидія промисловому шпигунству
10. Класифікація методів конкурентної розвідки
11. Поняття, характерні особливості та ознаки дезінформації
12. Місце й роль конкурентної розвідки в стратегічному проектуванні інформаційної безпеки підприємства
13. Людина як агент загрози конфіденційності на підприємстві. Методи мотивування людей до збереження конфіденційної інформації.
14. Зміст інформаційно-аналітичної діяльності конкурентної розвідки
15. Засоби інформаційно-аналітичної роботи конкурентної розвідки
16. Рівні та форми інформаційно-аналітичної діяльності, критерії оцінки інформації
17. Етапи інформаційно-аналітичної роботи
18. Порядок підготовки аналітичних документів
19. Відкриті джерела інформації в інформаційно-аналітичній роботі конкурентної розвідки

Література

1. Інформаційна безпека держави. Т. 1 / за заг. Ред.. В.В. Остроухова. – К. : ДНУ

«Книжкова палата України», 2016. – 264 с.

2. Інформаційна безпека держави. Т. 2 / за заг. Ред.. В.В. Остроухова. – К. : ДНУ «Книжкова палата України», 2016. – 328 с.

3. Хорошко В. А., Шелест М. Е. Информационно-аналитическое обеспечение безопасности. – К. : ВПП»Задруга», 2016. – 183 с.

4. Богуш В.М., Довидьков О.А., Кривуца В.Г. Теоретичні основи захищених інформаційних технологій. – К. : ДУІКТ, 2010. – 454 с.

5. Голубенко О.О., Хорошко В.О.,Петров О.С., Головань С.М., Яремчук Ю.Є. Політика інформаційної безпеки. Практикум. - Луганськ: Вид-во СНУ ім. В. Даля, 2010. – 208 с.

6. Ткачук Т.Ю. Конкурентна розвідка : навч. посіб. / Т.Ю. Ткачук. – К. : НА СБ України, 2010. – 219 с.

7. Ортинський В. Л., Керницький І. С, Живко З. Б. Економічна безпека підприємств, організацій та установ. - К. : Правова єдність, 2009.

8. Кавун С. В. Інформаційна безпека. - Х. : Вид. ХНЕУ, 2009. – 368 с.

9. Правове забезпечення інформаційної діяльності в Україні / За ред. Ю.С. Шемшученка, І.С. Чижа. - К. : ТОВ "Вид-во "Юридична думка", 2006. – 384 с.

10. Богуш В. М., Юдін О. К. Інформаційна безпека держави . - К. : "МК Прес", 2005. – 432 с.

11. Козаченко Г. В., Пономарьов В.П., Ляшенко О. М. Економічна безпека підприємства : сутність та механізм забезпечення : монографія. - К. : Лібра, 2003. – 280 с.

12. Гулак Г.М., Мухачов В.А.,Хорошко В.О., Яремчук Ю.Є. Основи криптографічного захисту інформації. - Вінниця: ВНТУ ,2011.-199с.

13. Хорошко В.О., Азаров О.Д., Шелест М.Є., Яремчук Ю.Є. Основи комп'ютерної стеганографії. - Вінниця: УНІВЕРСУМ.- 2003.-143с

14. Яремчук Ю.Є. Криптографічні методи та засоби шифрування інформації на основі рекурентних послідовностей. - Вінниця: Книга-Вега, 2002.-136с.

15. Вертузаєв М.С., Юрченко О.М. Захист інформації в комп'ютерних системах від несанкціонованого доступу: Навчальний посібник. – К.: Вид-во Європ. ун-ту, 2001. – 321 с.

16. Коваленко М. М. Комп'ютерні віруси і захист інформації : Навчальний посібник. - Національна академія внутрішніх справ України. – К.: Наукова думка, 1999. – 266 с.

17. Про національну програму інформатизації : Закон України від 04 лютого 1998 р. № 74/98.

18. Про державну таємницю : Закон України від 21 січня 1994 р. № 3855.

19. Про основи національної безпеки України : Закон України від 19 червня 2003 р. № 964.