ПРОГРАМА
вступного іспиту зі спеціальності
125 «Кібербезпека»
для вступників на навчання в аспірантурі

В програмі відображені наступні розділи теоретичних та практичних основ кібербезпеки та захисту інформації:

1. Методи та засоби захисту інформації;
2. Системи технічного захисту інформації;
3. Захист каналів зв'язку;
4. Методи та засоби контролю та спецвимірювань;
5. Методи та засоби стеганографії та криптографічного захисту інформації;
6. Організаційно-правове забезпечення інформаційної безпеки;
7. Аудит та менеджмент інформаційної безпеки.

1. Методи та засоби захисту інформації:

а) Класифікація і характеристика методів і засобів захисту інформації від витоку по технічним каналах;

б) Виявлення портативних електронних пристроїв перехоплення інформації: спеціальні обстеження, спеціальна перевірка. Пасивні та активні технічні заходи;

в) Екранування технічних засобів. Заземлення технічних засобів. Фільтрація інформаційних сигналів. Просторове та лінійне зашумлення.

г) Пасивні та активні методи і засоби захисту мовної інформації. Акустичне та віброакустичне маскування. Виявлення та придушення диктофонів і акустичних закладок;

д) Пасивні та активні методи захисту телефонних ліній. Методи маскуючи завад. Приклади технічної реалізації засобів захисту телефонних ліній та їх характеристики.

2. Системи технічного захисту інформації:

а) Системний підхід до технічного захисту інформації. Види інформації, що захищається. Демаскуючі ознаки об'єктів захисту;

б) Види загроз безпеці інформації. Джерела загроз безпеці інформації. Технічні канали просочування інформації;

в) Методи технічного та фізичного захисту інформації. Методи протидії спостереженню;

г) Методи протидії прослуховуванню. Виявлення та придушення закладних пристроїв;

д) Методи запобігання несанкціонованому запису мовної інформації. Системи технічного захисту інформації;

е) Периметральні системи охорони об'єктів. Системи відео нагляду та контролю доступу;

ж) Біометричні системи аутентифікації. Охоронні системи;

3.Захист каналів зв'язку:

а) Канали зв’язку і їх характеристики. Математичні моделі каналів зв’язку. Аналого-цифрове і цифро-аналогове перетворення в цифрових системах зв’язку. Дискретизація сигналів**;**

б) Амплітудна модуляція з подавленою несучою. Детектування модульованих сигналів з подавленою несучою. Частотна і фазова модуляція. Види імпульсної модуляції. Амплітудно-імпульсна та кодо-імпульсна модуляція;

в) Множинний доступ з частотним розділенням**.** Множинний доступ з часовим розділенням**.** Множинний доступ з частотно-часовим розділенням. Множинний доступ з кодовим розділенням;

г) Аспекти застосування принципів системного підходу до захисту інформації в каналах, мережах, системах зв’язку**.** Ієрархічна структура захисту інформації у предметній сфері зв’язку;

д) Організаційні аспекти захисту інформації в каналах зв’язку**.** Методи захисту мовної інформації в каналі зв’язку: накладання захисного шуму, частотні перетворення, перетворення в код з шифруванням, комбіновані мозаїкові перетворення;

е) Захист мовної інформації в каналі зв’язку: перетворення з інверсією спектру і статичними перестановками спектральних компонент мовного сигналу. Захист мовної інформації: перетворення з часовими перестановками (скремблюванням) і часовою інверсією елементів мовного сигналу. Захист мовної інформації: перетворення з часовими або частотними перестановками (скремблюванням). Захист мовної інформації за допомогою маскувальників;

ж) Аналіз проблеми захисту інформації в каналах на фізичному, канальному, системному рівнях. Фізичний, канальний, мережений, системний рівні захисту інформації в каналах стаціонарного, стільникового, супутникового зв’язку;

4. Методи та засоби контролю та спец вимірювань:

а) Похибки вимірювань фізичних величин. Аналогові вимірювальні прилади;

б) Цифрові вимірювальні прилади. Мікропроцесорні ЦВП;

в) Радіоприймальні вимірювальні прилади загального призначення. Спеціальні радіоприймальні прилади;

г) Індикатори електромагнітного випромінювання.Нелінійні локатори;

д) Автоматизовані пошукові комплекси. Доглядова техніка;

е) Планування радіоконтролю в Україні. Нормативні та методичні документи в галузі радіозв’язку;

5. Методи та засоби стеганографії:

а) Вбудова повідомлень у незначущі елементи контейнера. Математична модель стегосистеми та стеганографічні протоколи. Атаки на стегосистеми;

б) Пропускна здатність каналів передавання прихованої інформації: приховане перетворення, прихована пропускна здатність противника під час активної протидії зловмисника;

в) Основна теорема інформаційного збереження під час активної протидії зловмисника; властивості прихованої пропускної здатності стегоканалу; двійкова стегосистема передавання прихованих повідомлень;

г) Теоретико-ігрове формулювання інформаційно-прихованої протидії; використання контейнера як ключа стегосистеми; побудова декодера стегосистеми; аналіз випадку малих спотворень стего;

д) Приховування даних у просторої області зображень. Методи приховування в найменш значущому біті даних, блокове приховування, метод квантування, метод «хреста»;

е) Зберігання даних в аудіосигналах: методи кодування з розширенням спектру; вбудовування інформації у фазу сигналу; використання для вбудови ехо-сигналу; методи маскування системи цифрових водяних знаків;

ж) Приховування даних у відеопослідовностях з використанням стандарту MPEG, а також методи вбудовування інформації на рівні коефіцієнтів;

з) Методи вбудовування інформації бітової площини. Методи вбудовування інформації за рахунок енергетичної різниці між коефіцієнтами. Методи вбудовування інформації в текстових файлах.

6. Криптографічний захист інформації:

а) Класичні алгоритми криптографії. Алгоритми заміни та перестановки. Класичні алгоритми крипто аналізу. Частотний крипто аналіз;

б) Сучасні алгоритми симетричного шифрування. Стандарти DES, ГОСТ, AES;

в) Основні обчислювальні алгоритми симетричних криптосистем; Основні алгоритми крипто аналізу симетричних шифрів. Засоби симетричної криптографії;

г) Концепція відкритого ключа. Розподіл ключів в асиметричних криптосистемах;

д) Важкооборотні функції як основа асиметричних криптосистем;

е) Асиметрична система Рабіна. Основні алгоритми і засоби реалізації;

ж) Асиметрична система RSA. Основні алгоритми і засоби реалізації;

з) Основні криптографічні протоколи і засоби їх реалізації;

и) Електронний цифровий підпис;

к) Генератори випадкових і псевдовипадкових чисел.

7. Організаційно-правове забезпечення інформаційної безпеки:

а) Стандарти в галузі інформаційної безпеки;

б) Адміністративний рівень інформаційної безпеки;

в) Керування ризиками в галузі інформаційної безпеки;

г) Форми представлення інформації та їх характеристика;

д) Процедурний рівень інформаційної безпеки;

е) Забезпечення конфіденційності інформації;

ж) Організаційні заходи захисту інформації від витоку ТКВІ;

8. Аудит та менеджмент інформаційної безпеки:

а) Принципи забезпечення безпеки інформації в інформаційно - телекомунікаційних системах. Види аудиту безпеки інформаційних систем.

Загальні положення щодо захисту інформації в комп’ютерних системах від несанкціонованого доступу;

б) Практичні кроки аудиту інформаційної безпеки. Комплексний аналіз інформаційної системи організації та підсистеми Інформаційної безпеки на методичному, організаційно - управлінському, технологічному та технічному рівнях;

в) Стандарти в галузі аудиту інформаційної безпеки. Планування аудиту інформаційної безпеки організації. Управління аудитом інформаційної безпеки організації. Методики проведення;

г) Відпрацювання звітних документів при проведенні аудиту безпеки інформаційних систем підприємства;

д) Поняття ризику. Передумови для управління ризиками. Оцінювання ризиків як основа корпоративного управління. Оцінювання ризику. Кількісний та якісний аналіз ризиків. Інформаційна складова бізнес-ризиків;

е) Політика управління інформаційними ризиками. Структура системи управління ризиками. Неперервна діяльність з управління ризиками. Аутсорсинг процесів управління ризиками;

ж) Формулювання проблеми оцінювання та оброблення ризиків. Ідентифікація активів. Опис бізнес-процесів. Ідентифікація вимог інформаційної безпеки. Цінність інформації та активів;

з) Процес оброблення ризиків. Способи оброблення ризиків інформаційної безпеки. Оцінювання повернення інвестицій в інформаційну безпеку. Прийняття рішення про оброблення ризику. План оброблення ризиків;

и) Ідентифікація, аутентифікація, авторизація та підзвітність. моделі управління доступом. Техніки та технології управління доступом. Типи управління доступом. Аналіз сучасних моделей доступу. Довіра та гарантії.

ЛІТЕРАТУРА

1. Хорошко В.О., Азаров О.Д., Шелест М.Є. Основи копмп'ютерної стеганографії. Навч.посібн. для студентів і аспірантів. – Вінниця: ВДТУ, 2003.- 143 с.

2. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография М.: СОЛОН-Пресс, 2002.

3. Конахович Г.Ф., Пузыренко А.Ю. Комп'ютерная стеганографія. Теория и практика. – К.: «МК-Пресс», 2006. – 288 с.

4. Кузнецов О.О. Стеганографія: навч.посібн. / О.О.Кузнецов, С.П.Євсеєв, О.Г.Король. – Х.:Вид.ХНЕУ, 2011.— 232 с.

5. Дж.Миано Форматы и алгоритмы сжатия изображений в действии. Уч.пособие. – М.: Изд. «Триумф», 2003. – 336 с.

6. Дудикевич В. Б. Захист засобів і каналів телефонного зв’язку: Навчальний посібник / В. Б. Дудикевич, В. В. Хома, Л. Т. Пархуць. – Л.: Видавництво Львівської політехніки, 2012. – 210 с.

7. Радиосистемы и сети передачи информации / Н.А.Важенин, В.А.Вейцель, А.С.Волковский, Р.Б.Мазепа, Б.В.Рощин, Е.А.Симаков, А.Г.Терехин, А.И.Фомин. – М.: Издательство МАИ, 2002.

8. Скляр Бернард. Цифровая связь. Теоретические основы и практическое применение. – М.: Изд. Дом “Вильяме”. – 2003. – 1104 с.

9. Алхимов Ю .В. Современные коммуникационные системы: учебное пособие / Ю. В. Алхимов, В. К. Кулешов. – Томск: Изд. ТПУ, 2008. – 200 с.

10. Дудикевич В. Б., Концептуальні моделі захисту інформації для технологій стаціонарного, стільникового, супутникового зв’язку / В. Б. Дудикевич, Ю. Р. Гарасим, Г. В. Микитин // Вісник Національного університету “Львівська політехніка”, Автоматика, вимірювання та керування. – 2010. – №665. – С. 18–26.

11. Защита беспроводных телекоммуникационных систем: учеб. пособие / [В. Б. Щербаков, А. В. Гармонов, С. А. Ермаков и др.]. – Воронеж: ФГБОУ ВПО “Воронежский государственный технический университет”, 2013. – 127 с.

12. Петренко С.А. Политики информационной безопасности./ Петренко С.А., Курбатов В. А. — М.: Компания айти, 2006. — 400 с

13. Хорошко В.А.Методы и средства защиты информации/ Хорошко В.А., Чекатков А.А. - К.: Юниор, 2003. - 504с.

14. Домарев В.В. "Безопасность информационных технологий. Методология создания систем защиты"/ Домарев В.В. – К.: ООО "ТИД "ДС", 2002 – 688 с.

15. Ленков С.В. Методы и средства защиты информации. В 2-х томах. Том 1. Несанкционированное получение информации/ Перегудов Д.А., Хорошко В.А., под ред. В.А. Хорошко.– К.: Арий, 2008. -464 с., ил.

16. НД ТЗІ 1.4-001-2000: «Типове положення про службу захисту інформації в автоматизованій системі» від 4 грудня 2000 р. № 53 із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806.

17. ДСТУ 3396.1-96: «Захист інформації. Технічний захист інформації. Порядок проведення робіт». Чинний від 01.07.1997 р.

18. ДСТУ ГОСТ 28147-2009. Системи обробки інформації. Захист криптографічний. Алгоритм криптографічного перетворення (ГОСТ 28147-89). – Чинний від 2009-02-01. – Київ : Держстандарт України, 2009.

19. Олійников Р. Принципи побудови і основні властивості нового національного стандарту блокового шифрування України / Р. Олійников, І Горбенко, О. Казимиров [та ін.] // Захист інформації.– квітень - червень 2015.– № 2.– С. 142-157.

20. Совин Я. Р. Ефективна реалізація алгоритму ДСТУ ГОСТ 28147-89 для 8-16-32-бітних вбудованих систем / Я. Р. Совин, В.В. Хома, І. Я. Тишик [та ін.] // НУ “Львівська політехніка”, Львів.

21. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Теорія і практика. Застосування: монографія.–Харків: Видавництво «Форт», 2012.–870с.

22. Горбенко Ю.І., Горбенко І.Д. Інфраструктура відкритих ключів. Електронний цифровий підпис. Теорія та практика: монографія.–Харків: Видавництво «Форт», 2010.–608с.