

Інститут комп'ютерних технологій, автоматики та метрології

Спеціалізація:

Кібербезпека

(код 125/0210)

Спеціальність:

Адміністративний менеджмент у сфері захисту інформації

(код 125)

Галузь знань:

Інформаційні технології

(код 12)

Перелік дисциплін

для вступу на навчання за освітньою програмою підготовки магістр

- **Алгоритмічні мови та програмування**
- **Інформаційно-аналітичне забезпечення безпеки**
- **Методи і засоби захисту інформації**
- **Системний аналіз інформаційної безпеки**
- **Технічні засоби охорони об'єктів**

Дисципліна: Алгоритмічні мови та програмування

Розділ 1. Алгоритмічна мова С#

- § 1. Елементарні типи даних.
- § 2. Базові вирази та оператори.
- § 3. Об'єктно-орієнтоване програмування.

Розділ 2. Алгоритмічна мова Сі.

- § 1. Елементи мови Сі.
- § 2. Оголошення.
- § 3. Операції та вирази.
- § 4. Оператори.
- § 5. Функції.
- § 6. Директиви препроцесору та вказівки компілятору.

Література

1. Шилдт Г. С# : учеб. курс : пер. с англ. / Г. Шилдт. – СПб. : Питер; К. : изд. группа BHV, 2003.
2. Марченко А.Л. Основы программирования на С# 2.0 / А.Л. Марченко. – М. : ИНТУИТ.РУ, 2007.
3. Керниган Б. Язык программирования Си. Задачи по языку Си : пер. с англ. / Б. Керниган, Д. Ритчи, А. Фьюэр. – М. : Финансы и статистика, 1985.

Дисципліна: Інформаційно-аналітичне забезпечення безпеки

Розділ 1. Вступ. Мета і завдання курсу. Основні положення політики забезпечення інформаційної безпеки

§ 1. Вимоги стандарту щодо забезпечення інформаційної безпеки. Наслідки у випадку порушення політики безпеки

Розділ 2. Організаційні заходи щодо забезпечення безпеки

- § 1. Класифікація і управління ресурсами. Безпека персоналу та фізична безпека
- § 2. Відповідність інформаційної системи до вимог стандарту
- § 3. Управління комунікаціями і процесами та контроль доступу
- § 4. Сучасні методи та засоби мережного захисту

Розділ 3. Концепції та моделі безпеки інформаційних технологій

§ 1. Процес керування безпекою інформаційних технологій. Елементи безпеки

Розділ 4. Керування та планування безпеки інформаційних технологій. Методика безпеки інформаційних технологій

- § 1. Організаційні аспекти. Вибір стратегії аналізу ризику
- § 2. Методика та рекомендації щодо захисту інформаційних технологій
- § 3. Впровадження захисту. Механізм доопрацювання
- § 4. Методи керування захистом інформаційних технологій
- § 5. Цілі, стратегії методики безпеки інформаційних технологій. Застосування плану безпеки інформаційних технологій
- § 6. Варіанти стратегії аналізування ризику

Розділ 5. Вступ до вибору засобів захисту та концепція базової безпеки

- § 1. Засоби захисту та базове оцінювання
- § 2. Вибір засобів захисту відповідно до типу системи
- § 3. Вибір засобів захисту відповідно до загроз безпеці
- § 4. Вибір засобів захисту відповідно до детальних оцінок
- § 5. Розроблення базової безпеки організації

Розділ 6. Настанова з керування мережною безпекою

- § 1. Огляд вимог політики інформаційної безпеки щодо мережних архітектур і програм
- § 2. Огляд характеристик мережі та співвідношення, пов'язані з довірою
- § 3. Визначення типів ризиків безпеки. Визначення відповідних потенційних сфер застосування засобів захисту
- § 4. Документування та перегляд варіантів архітектури безпеки

Література

1. Нормативне забезпечення інформаційної безпеки / С.М. Головань, О.С. Петров, В.О. Хорошко та ін. – К. : ДУІКТ, 2008.
2. Давыдов Н. Информационно-аналитическое обеспечение фирмы / Н. Давыдов // Служба безопасности. – 2000. – № 3-4.
3. Кузнецов Н. Учебник по информационно-аналитической работе / Н. Кузнецов. – М. : Яуза, 2000.

Дисципліна: Методи і засоби захисту інформації

Розділ 1. Основні форми представлення інформації

- § 1. Мовна (акустична) форма представлення інформації
- § 2. Документальна форма представлення інформації
- § 3. Телекомунікаційна форма представлення інформації

Розділ 2. Основні об'єкти захисту інформації

- § 1. Поняття контрольованої зони
- § 2. Небезпечні зони
- § 3. Випадкові антени
- § 4. Види інформаційних сигналів

Розділ 3. Технічні канали витоку інформації

- § 1. Технічні канали витоку інформації
- § 2. Технічні канали витоку телекомунікаційної інформації
- § 3. Технічні канали витоку акустичної інформації

Розділ 4. Класифікація методів і засобів захисту інформації від витоку технічними каналами

- § 1. Організаційні заходи
- § 2. Технічні заходи
- § 3. Спеціальні обстеження та перевірка

Розділ 5. Методи і засоби захисту інформації ТЗПІ від витоку технічними каналами

- § 1. Пасивні методи захисту
- § 2. Активні методи захисту

Розділ 6. Екранування технічних засобів

- § 1. Електростатичне екранування
- § 2. Магнітостатичне екранування
- § 3. Електромагнітне екранування
- § 4. Матеріали для виготовлення екранів
- § 5. Екранування сполучних ліній
- § 6. Екранування приміщень

Розділ 7. Заземлення технічних засобів

- § 1. Схеми заземлення
- § 2. Основні вимоги до системи заземлення
- § 3. Опір заземлення

Розділ 8. Фільтрація інформаційних сигналів

- § 1. Роздільні трансформатори
- § 2. Завадопоглинальні фільтри
- § 3. Основні вимоги до захисних фільтрів

Розділ 9. Просторове і лінійне зашумлення

- § 1. Вимоги до систем зашумлення

§ 2. Генератори шуму

§ 3. Системи лінійного зашумлення

Розділ 10. Методи і засоби захисту мовної інформації

§ 1. Пасивні методи захисту акустичної (мовної) інформації

§ 2. Активні методи захисту акустичної (мовної) інформації

Розділ 11. Звукоізоляція приміщень

§ 1. Звукоізоляція приміщень

§ 2. Звукоізоляція дверей

§ 3. Звукоізоляція вікон

§ 4. Звуковбирні матеріали

Розділ 12. Акустичне маскування

§ 1. Генератори акустичного шуму

§ 2. Придушувачі диктофонів і акустичних закладок

Розділ 13. Методи і засоби захисту телефонних ліній

§ 1. Пасивні методи захисту телефонних ліній

§ 2. Активні методи захисту телефонних ліній

§ 3. Пристрої активного захисту телефонних ліній

§ 4. Пристрої контролю телефонних ліній

§ 5. Блокування роботи телефону

Література

1. Хорошко В.А. Методы и средства защиты информации /В.А. Хорошко, А.А. Чекатов. – К. : ЮНИОР, 2003. – 504 с.

2. Максименко Г.А. Методы выявления, обработки и идентификации сигналов радиозакладных устройств / Г.А. Максименко, В.А. Хорошко. – К. : Полиграф Консалтинг, 2004. – 317 с.

3. Ленков С.В. Методы и средства защиты информации : в 2 т. / С.В. Ленков, Д.А. Перегудов, В.А. Хорошко. – К. : Арий, 2008. – Т. 1 : Несанкционированное получение информации – 464 с.; Т. 2 : Информационная безопасность. – 344 с.

Дисципліна: Системний аналіз інформаційної безпеки

Розділ 1. Вступ. Мета та завдання системного аналізу інформаційної безпеки

§ 1. Мета та завдання системного аналізу інформаційної безпеки. Роль предмета у формуванні спеціаліста з інформаційної безпеки

Розділ 2. Методи захисту інформації в комп'ютерних системах та мережах

§ 1. Загрози безпеки інформаційним системам

§ 2. Типи атак на протоколи взаємодії

§ 3. Служба захисту. Короткий огляд методів захисту

§ 4. Ознайомлення з нормативно-правовими документами та державними стандартами щодо захисту інформаційної безпеки

Розділ 3. Електронний бізнес та проблеми безпеки корпоративних інформаційних систем

§ 1. Глобальна мережа Internet

§ 2. Електронний бізнес в Internet та здійснення електронних платежів

§ 3. Основні моделі електронної комерції та проблеми безпеки корпоративних інформаційних систем

Розділ 4. Методи та засоби отримання інформації щодо банківської діяльності.

Комерційна таємниця банків та організація її захисту

§ 1. Джерела конфіденційної інформації та технічні канали витоку інформації в банківській діяльності

§ 2. Легальні та напівлегальні методи збору інформації

§ 3. Принципи організації та роботи дозвільної системи банку

§ 4. Системний аналіз, проектування, побудова та управління комплексною системою інформаційної безпеки комерційної таємниці банків

Розділ 5. Ризики у банківській діяльності. Тенденції розвитку в побудові комплексних систем інформаційної безпеки

- § 1. Класифікація ризиків, їх аналіз та методологія
- § 2. Тенденції розвитку в побудові комплексних систем інформаційної безпеки
- § 3. Інтеграція систем інформаційної безпеки та впровадження систем централізованого керування

Література

1. Гарасимчук О.І. Комплексні системи санкціонованого доступу : навч. посіб. / О.І. Гарасимчук, В.Б. Дудикевич, В.А. Ромака. – Львів : вид-во НУ «Львівська політехніка», 2010. – 212 с.
2. Катренко А.В. Системний аналіз об'єктів та процесів комп'ютеризації : навч. посіб. / А.В. Катренко. – Львів: Новий світ-2000, 2003 – 424 с.
3. Хорошко В.А. Методы и средства защиты информации / В.А. Хорошко, А.А. Чекатков. – К. : Юниор, 2003. – 504 с.
4. Шумский В.А. Системный анализ в защите информации: учеб. пособие для студ. вузов, обучающихся по спец. в обл. информ. безопасности / В.А. Шумский, А.А. Шелупанов. – М. : Гелиос АРВ, 2005. – 224 с.

Дисципліна: Технічні засоби охорони об'єктів

Розділ 1. Концепція захисту об'єктів з використанням технічних засобів охорони в сучасних умовах

§ 1. Тенденції розвитку сучасних систем безпеки. Загальні вимоги до створення ефективних систем безпеки об'єктів охорони. Методика вибору раціональних варіантів захисту об'єкта з використанням технічних засобів охорони

Розділ 2. Теоретичні основи захисту і технічної охорони об'єктів

§ 1. Структура системи охорони об'єктів. Тактики охорони об'єктів. Принцип послідовності рубежів

§ 2. Природні і штучні перешкоди. Види природних і штучних перешкод. Методи захисту природних і штучних перешкод. Структура типового комплексу технічних засобів охорони об'єктів

Розділ 3. Засоби сповіщення в технічних засобах охорони об'єктів

§ 1. Сповіщувачі тривожної сигналізації. Класифікація сповіщувачів. Застосування і принципи дії

§ 2. Сповіщувачі пожежної сигналізації. Основні характеристики, класифікація, застосування і принципи дії

Розділ 4. Засоби спостереження та відеоконтролю

§ 1. Засоби телевізійного спостереження. Структурна схема системи телевізійного спостереження. Склад і основні функції системи телевізійного спостереження

§ 2. Телевізійні камери. Корпусні і безкорпусні телевізійні камери. Камери на приладах із зарядовим зв'язком. Чутливість, що вирішує здатність. Телевізійні камери з постійною і змінною фокусною відстанню. Мініатюрні телекамери для прихованого спостереження

Розділ 5. Системи засобів нейтралізації загроз та захист об'єктів від проникнення

§ 1. Системи засобів нейтралізації загроз

§ 2. Тривожна сигналізація. Призначення тривожної сигналізації. Види тривожної сигналізації. Особливості різних видів тривожної сигналізації

Розділ 6. Засоби управління системою охорони

§ 1. Автоматизовані інтегровані системи охорони. Адресні панелі, виконавчі пристрої. Загальне управління системою охорони

Література

1. Дослідження охоронних систем відеоспостереження: інструкція до лабораторної роботи №2 з курсу «Елементи та пристрої фізичного та електронного захисту об'єктів» для студентів спеціальності 6.1601 «Інформаційна безпека» / укл.: О.І.Гарасимчук, З.М. Стрілецький. – Львів: НУ «ЛП», 2008. – 17 с.
2. Торокин А.А. Основы инженерно-технической защиты информации /А.А. Торокин. – М.: Ось-89, 1998. – 336 с.
3. Абалмазов Э.И. Методы и инженерно-технические средства противодействия информационным угрозам /Э.И. Абалмазов. – М.: Компания «Гротек», 1997. – 246 с.
4. Каторин Ю.Ф. Большая энциклопедия промышленного шпионажа /Ю.Ф. Каторин и др. – СПб.: Полигон, 2000. – 896 с.
5. Андрианов В.И. Охранные устройства для дома и офиса / В.И. Андрианов, А.В.Соколов. – СПб.:

Лань, 1997. – 304 с.