

Перелік питань для підготовки до вступних іспитів в аспірантуру
зі спеціальності 125 Кібербезпека та захист інформації

Вступний іспит із спеціальності складається в обов'язі програми вищої освіти магістра з відповідної спеціальності (п. 20 Порядку підготовки здобувачів вищої освіти ступеня доктора філософії та доктора наук у закладах вищої освіти (наукових установах), затвердженого постановою Кабінету Міністрів України від 23 березня 2016 р. № 261).

Перелік питань для підготовки до вступних іспитів зі спеціальності 125 Кібербезпека та захист інформації укладено на підставі таких програм навчальних дисциплін:

1. Управління доступом до інформаційних ресурсів.
 2. Моніторинг та аудит інформаційно-комунікаційних систем.
 3. Криптологія.
 4. Аналіз шкідливого коду.
 5. Інтернет речей: безпека та приватність.
-
1. Методи передавання, що забезпечують енергетичну прихованість сигнальних конструкцій в каналі. Шумоподібні сигнали та методи їх формування. Умови забезпечення енергетичної та структурної прихованості.
 2. Основні параметри блокових коректувальних кодів. Загальний принцип декодування з виявленням та виправленням помилок. Оцінка здатності кодів виявляти та виправляти помилки.
 3. Взаємозв'язок між енергетичною та частотною ефективністю системи зв'язку при забезпеченні прихованості передавання сигнальних конструкцій. Забезпечення енергетичної прихованості пояснити на основі теореми Шеннона про пропускну здатність.
 4. Технології доступу на основі радіочастотної ідентифікації NFC та RFID. Фізичні принципи взаємодії та протоколи передавання даних. Загрози та шляхи їх вирішення.
 5. Захист інформації в умовах радіоелектронної боротьби (РЕБ). Завадозахищеність систем передавання. Поняття завадостійкості та прихованості. Енергетична, структурна та інформаційна прихованість.
 6. Теорема Шеннона для каналу без завад. Методи ефективного кодування джерел дискретних повідомлень. Коди Шеннона-Фано, Хаффмана та арифметичні коди.
 7. Поняття моделі керування доступом. Дискреційне, мандатне та рольове керування доступом.
 8. Кіберсередовище. Кібербезпека та її задачі. Технології, служби, послуги та механізми кібербезпеки. Архітектура кібербезпеки. Політика безпеки.
 9. Перелік загроз кібербезпеці за Рекомендаціями МСЕ-Т X.800, X.805. Порядок оцінки загроз. Аналіз вразливостей. Описання та аналіз загроз.
 10. Структура безпеки мережі з кінця в кінець за Рекомендацією МСЕ-Т X.805. Вісім послуг безпеки, що захищають від атак та основних загроз безпеки.
 11. Рівні ієрархії мережного обладнання: рівень безпеки інфраструктури, рівень безпеки послуг, рівень безпеки застосувань.
 12. Вимоги гарантії конфіденційності, цілісності й точності (вірності) передавання даних мережею. Застосування шифрування та хешування інформації для забезпечення безпеки. Методи захисту між точками доступу локальної мережі.
 13. Модель забезпечення безпеки центру управління мережею. Єдина структура захисту мережі. Послуги безпеки у технології безпеки управління мережею.

14. Визначення контролю доступу. Технології захисту периметра: фільтрація змісту даних, міжмережеві фільтри, приховування адрес мережі, шлюзи рівнів застосувань, проксі-застосування.
15. Віртуальна приватна мережа (VPN): віддалений доступ з VPN, типи VPN, VPN рівня 2, 3, 4, тунелі як тракти передачі даних, послуги безпеки VPN.
16. Автентифікація: методи автентифікації, категорії систем автентифікації – одно-факторні, двох-факторні, три-факторні системи автентифікації; смарт-картки; сильна автентифікація, що ґрунтується на шифруванні.
17. Ідентифікація: категорії ідентифікації, рольовий принцип ідентифікації, ідентифікація на основі правил.
18. Сканування на наявність вірусів. Антивірусні технології. Метод сигнатур. Методи забезпечення цілісності системи.
19. Методи віддаленого доступу. Основні загрози віддалених користувачів. Технології та послуги віддаленого доступу: комутованого доступу до централізованого вузлу підприємства, мережі VPN віддаленого доступу, мережі VPN на основі IPSec. Механізми захисту віддаленого доступу.
20. Вразливості мереж WLAN. Інфраструктура мереж WLAN. Загрози мережам WLAN. Механізми та вимоги до безпеки бездротової точки доступу. Багаторівневий підхід до організації захисту бездротових мереж LAN.

Гарант освітньо-наукової програми
третього (освітньо-наукового) рівня вищої освіти
зі спеціальності 125 Кібербезпека та
захист інформації



Євген ВАСІЛІЙ