МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖУЮ
Проректор з наукової роботи
_____ Микола ДИВАК

ПРОГРАМА

проведення фахового вступного випробування
для претендентів на здобуття
третього (освітньо-наукового) рівня вищої освіти
зі спеціальності 125 Кібербезпека та захист інформації

Заслухано на засіданні приймальної комісії
протокол № 3 від 28 березня 24 р.

Тернопіль
2024

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

Програма вступного іспиту зі спеціальності 125 «Кібербезпека та захист інформації» для підготовки за науковим ступенем доктор філософії складена відповідно до нормативних вимог цієї спеціальності.

Мета проведення іспиту – визначення рівня знань, умінь і навичок претендентів та їх відбір на конкурсній основі.

Теоретичні питання вступного іспиту складаються із чотирьох розділів:

1. Криптографічні методи та протоколи
2. Безпека комп'ютерних мереж
3. Системи технічного захисту інформації
4. Системи та технології кібербезпеки

2. ТЕМИ, ЩО ВИНОСЯТЬСЯ НА ВСТУПНЕ ВИПРОБОВУВАННЯ

2.1 Криптографічні методи та протоколи

1. Шифри перестановки та простої заміни. Принципи криптографічного захисту інформації. Криптоаналітичні атаки. Їх види. Шифр скитала. Шифруючі таблиці. Шифр магічних квадратів. Шифр Кардано. Шифр атбаш. Полібіанський квадрат. Шифр Цезаря. Шифр Цезаря з ключовим словом. Шифруючі таблиці Трисемуса. Шифри складної заміни. Шифр одноразового блокноту.

2. **Шифр Гронсфельда.** Шифр Гронсфельда з ключовим словом. Шифр Віженера. Шифр Віженера з ключовим словом. Роторні шифрувальні машини. Роторна шифрувальна машина Enigma. Біграмний шифр Плейфейра. Подвійний квадрат Уїтстона. Шифр чотирьох квадратів. Шифр ADFGVX. Шифр одноразового блокноту. Алгоритм DES.

3. **Структура алгоритму DES.** Його переваги та недоліки. Операції алгоритму DES. Функція шифрування алгоритму DES. Генерація підключів алгоритму DES. Режими роботи алгоритму DES: електронна кодова книга, зчеплення блоків шифру, зворотній зв’язок по шифртексту, зворотній зв’язок по виходу. Галузі застосування алгоритму DES.

4. **Алгоритми IDEA та ГОСТ28147–89.** Структура алгоритму IDEA. Його переваги та недоліки. Операції алгоритму IDEA. Генерація підключів алгоритму IDEA. Загальна структура алгоритму ГОСТ28147–89. Його переваги та недоліки.

5. **Український та світовий стандарти симетричного шифрування.** Український стандарт симетричного шифрування «Калина». Світовий стандарт симетричного шифрування AES (Rijndeal). **Сімейство алгоритмів RC**. RC-подібні алгоритми. Алгоритми RC 2, RC 4, RC 5, RC 6.

6. **Арифметика асиметричних криптосистем**. Основні поняття. Алгоритм Евкліда, його наслідок, пошук оберненого елемента, китайська теорема про остачі. Функція Ейлера. Теореми Ейлера та Ферма.

7. **Криптосистема RSA.** Опис криптосистеми RSA. Генерування ключів. Шифрування та розшифрування. Коректність, ефективність та надійність криптосистеми.

8. **Криптосистема Рабіна.** Генерування ключів криптосистеми Рабіна. Шифрування та розшифрування в криптосистемі Рабіна. Коректність, ефективність та надійність криптосистеми.

9. **Криптосистема Ель–Гамаля.** Криптосистема Ель–Гамаля. Шифрування та розшифрування в криптосистемі Ель–Гамаля. Коректність, ефективність та надійність криптосистеми.

10. Електронний цифровий підпис. Поняття електронного цифрового підпису. Електронний цифровий підпис в системах RSA та Ель–Гамаля. Алгоритм DSA. Система Шнорра. Ефективність, достовірність та конфіденційність підписів у різних алгоритмах.

11. **Шифрування із паролем.** Шифрування із паролем. Апаратні пристрої збереження ключів. Криптографічні акселератори. Біометрична ідентифікація.

12. **Поняття хеш-функції. Застосування хеш-функцій.** Визначення функції хешування та вимоги до неї. Алгоритм функції хешування по ГОСТ Р 34.11-94. Аналіз алгоритму та особливостей його програмної реалізації. Геш-функції на основі ділення. Мультиплікативна схема гешування. Гешування рядків змінної довжини. Криптографічні хеш-функції. Геометричне гешування. Прискорення пошуку даних.

13. **Хеш-функції типу MD та SHA. Український стандарт хешування.** Хеш-функція MD (MD-2, MD-4, MD-5). Сімейство хеш-функцій SHA (SHA-1, SHA-2, SHA-3, SHA-256). Український стандарт хешування ДСТУ 7564:2014 «Купина».

14. **Генерація ЕЦП на основі хеш-функцій.** Процедура вироблення та перевірки електронного підпису по ДСТУ 4145-2002. Генерація загальних параметрів, секретного та відкритого ключів. Особливості програмної реалізації процедури. Алгоритм DSA.

15. **Поняття еліптичної криптографії. Реалізація шифрування на еліптичних кривих.** Еліптичні криві над кінцевими полями. Еліптичні криві над полями непарної характеристики. Теорема Хассе. Еліптичні криві над полями характеристики 2. Проективні координати. Швидка редукція (NIST-криві). Еліптичні криві, рекомендовані NIST. Розмір ключа.

16. **ЕЦП на основі еліптичних кривих.** Особливості ЕЦП на основі еліптичних кривих. Вибір параметрів. Генерування ключів ECDSA. Переваги ECDSA перед DSA. Практична реалізація.

17. **Криптографічні протоколи.** Визначення криптографічного протоколу. Перелік вимог до криптографічного протоколу. Аналіз атак на криптографічні протоколи. Використання симетричного та несиметричного шифрування в криптографічних протоколах.

18. **Приклади сучасних комп'ютерних криптографічних систем.** Характеристики протоколу SSL компанії Netscape Communication Corporation для захисту інформаційного обміну в середовищі Інтернет. Ієрархія ключів, блок-схема розсилки ключів абонентам мережі, блок-схема забезпечення цифрового підпису даних в мережі.

19. **Елементи стеганографії.** Комп'ютерна стеганографія. Методи вкладення інформації у файли мультимедіа. Методи приховування інформації в зображеннях. Методи приховування інформації в аудіо сигналах.

20. **Квантова криптографія.** Поняття квантової криптографії. Квантовий розподіл ключів. Способи та пристрої генерації та передачі одиночних фотонів. Фазове та часове кодування. Основні напрямки розвитку та проблеми квантової криптографії. Порівняльний аналіз протоколів квантової криптографії.

Рекомендована література

1. Лісовська Ю. Кібербезпека. Ризики та заходи. - К.: Кондор, 2019. - 272 с.
2. Касянчук М. Досконала форма системи залишкових класів: методи побудови та застосування (Монографія) / М.Касянчук. – Тернопіль: ТНЕУ, 2019. – 224 с.
3. Тарнавський Ю.А. Технології захисту інформації [Електронний ресурс]: підручник. – К.: КПІ ім. Ігоря Сікорського, 2018. – 162 с. Режим доступу до ресурсу: https://ela.kpi.ua/bitstream/123456789/23896/1/TZI_book.pdf
4. Інформаційна безпека: навчальний посібник/ Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв та інші; за заг. ред. д-ра техн. наук, проф. Ю. Я. Бобала та д-ра техн. наук, доц. І.В. Горбатого. Львів : Видавництво Львівської політехніки, 2019. 580 с.
5. Криптоаналіз. Криптографічні протоколи. Навчальний посібник/ О.М. Гапак. Ужгород: Ужгородський національний університет, 2021. 93 с.

2.2 Безпека комп'ютерних мереж

1. Ідентифікація, аутентифікація і авторизація в комп'ютерних мережах
2. Тріада «конфіденційність, доступність, цілісність»
3. Типи і приклади атак на комп'ютерні мережі. Пасивні і активні атаки
4. Відмова в обслуговуванні.
5. Адміністративний рівень. Політика безпеки. Засоби безпеки процедурного рівня.
6. Технології автентифікації.
7. Фактори автентифікації людини. Автентифікація на основі паролів. Автентифікація на основі апаратних автентифікатор.
8. Автентифікація інформації. Електронний підпис. Автентифікація на основі цифрових сертифікатів.
9. Технології управління доступом і авторизації. Форми подання обмежень доступу.
10. Системи аутентифікації і управління доступом операційних систем.
11. Автентифікація в ОС сімейства Unix. Протокол SSH.
12. Технології безпеки на основі фільтрації і моніторингу трафіку. Види фільтрації трафіку.
13. Фаєрволи. Функціональне призначення брандмауера. Типи фаєрволів.
14. Проксі-сервери. Функції проксі-сервера.
15. Типові архітектури мереж, що захищаються фаєрволом.
16. Моніторинг трафіку. Аналізатори протоколів.
17. Системи виявлення вторгнень.
18. Архітектура мережі з захистом периметра і поділом внутрішніх зон. Аудит подій безпеки.
19. Атаки на транспортну інфраструктуру мережі. TCP-атаки. Затоплення SYN-пакетами. Підробка TCP-сегмента.
20. Мережева розвідка. Завдання і різновиди мережевої розвідки. Сканування мережі. Сканування портів.

Рекомендована література

1. Jason Callaway. COMPUTER NETWORKING: 2 BOOKS IN 1 – All You Need to Know to Become a Networking Engineer from Scratch (Wireless Technologies, Network System, IP subnetting, Cybersecurity, and much more) - (October 8, 2021), 181 pages.
2. Scott Jernigan, Mike Meyers. CompTIA Network+ Certification All-in-One Exam Guide, Eighth Edition (Exam N10-008) 8th Edition - (March 28, 2022), 976 pages.

3. Russell Scott. Computer Networking: This Book Includes: Computer Networking for Beginners and Beginners Guide (All in One) - (December 28, 2019), 359 pages.

4. Ramon Nastase. Computer Networking for Beginners: Your Guide for Mastering Computer Networking, Cisco IOS and the OSI Model (Computer Networking Series) Paperback – February 1, 2018, 188 pages.

5. Larry L. Peterson, Bruce S. Davie. Computer Networks: A Systems Approach (The Morgan Kaufmann Series in Networking) 6th Edition- (March 29, 2021), 848 pages.

2.3 Системи технічного захисту інформації

1. Види та носії інформації, що підлягають захисту. Класифікація джерел інформації. Види носіїв інформації: люди, документи, продукція, вимірювальні датчики, інтелектуальні засоби обробки інформації, чернетки і відходи виробництва, матеріали і технологічне обладнання. Сутність запису і знімання інформації з носія.

2. Небезпечні сигнали та їх джерела. Джерела сигналів. Джерела функціональних сигналів: передавачі радіо- і радіотехнічних засобів і систем, лазерні системи зв'язку, випромінювачі акустичних сигналів гідролокаторів і засобів підводного зв'язку, умовні сигнали. Побічні та паразитні електромагнітні випромінювання та наведення.

3. Технічні розвідки, їх можливості та застосування. Розвідувальна діяльність. Технічна розвідка. Основні принципи організації й ведення технічної розвідки. Класифікація іноземної технічної розвідки. Можливості видів технічної розвідки. Протидія технічним засобам розвідки.

4. Засоби відеоспостереження та пожежної сигналізації, їх характеристики. Системи охорони територій. Їх класифікація та характеристики. Системи сигналізації. Комбіновані системи охорони територій. Системи відкритого і прихованого відеоспостереження. Засоби пожежної сигналізації, їх характеристики.

5. Радіо- та електротехнічні канали витоку інформації. Фізичні основи радіо- та електротехнічних каналів. Структура та класифікація радіоканалів витоку інформації. Радіомоніторинг. Канали перехоплення (зняття) інформації з каналів зв’язку. Радіоелектронні канали витоку інформації.

6. Акустичні та віброакустичні канали витоку інформації. Фізичні основи акустики та віброакустики. Акустичні канали витоку інформації. Середовище поширення акустичних сигналів. Шляхи витоку акустичної інформації. Особливості віброакустичних каналів. Акустоелектричні канали. Оптико-електронний канал. Параметричні канали. Обладнання кімнати для переговорів.

7. Електричні канали витоку інформації. Фізичні основи електричних каналів витоку інформації. Канал побічних електромагнітних випромінювань ОТЗС. Канал побічних електромагнітних випромінювань ДТЗС. Канал

“паразитної” модуляції сигналів ВЧ генераторів. Канал “паразитної” ВЧ генерації підсилювачів. Канал побічних електромагнітних наведень на лінії електроживлення (заземлення) ОТЗС. Канал побічних електромагнітних наведень на комунікації ДТЗС. Канал ВЧ нав’язування (для зняття інформації, що обробляється в ОТЗС).

8. Візуально-оптичні та матеріально-предметні канали витоку. Фізичні основи оптичних каналів витоку інформації. Технічні канали витоку видової інформації. Загрози витоку видової інформації. Способи отримання видової інформації. Способи прихованого відеоспостереження і зйомки Матеріально-речовинні канали витоку інформації. Способи гарантованого знищення та добування інформації з магнітних носіїв.

9. Закладні пристрої. Канали витоку інформації на основі закладних пристроїв. Сутність та класифікація засобів несанкціонованого перехоплення інформації (закладних пристроїв). Радіозакладні пристрої. Радіозакладні пристрої з перевипромінюванням. Загальні характеристики та особливості деяких типів закладних пристроїв. Закладні пристрої типу «довге вухо» або закладка «зі штучно піднятою трубкою». Мережеві закладні пристрої. Заходи захисту інформації від витоку каналами на основі закладних пристроїв. Методи виявлення закладних пристроїв. Демаскуючі ознаки закладних пристроїв.

10. Технічні засоби пасивного та активного захисту мовної інформації. Спектр мовного сигналу. Спектри шумів. Зашумлення мовного сигналу. Перетворення спектра мовного сигналу (скремблювання сигналів). Пасивні засоби захисту. Організаційні та режимні заходи. Активні засоби захисту. Створення маскуючи та вібраційних перешкод. Лінійне зашумлення ліній електроживлення.

11. Застосування мобільних пристроїв для перехоплення інформації та засоби їх захисту. Склад мобільних пристроїв. Підслуховуючі пристрої з мобільним зв'язком. GSM підслуховуючий пристрій на основі мобільного телефона. Методи протидії підслуховуючим пристроям з мобільним зв’язком.

12. Придушення радіоканалів витоку інформації. Структурна схема радіомікрофона (РМ). Схемотехнічна реалізація аналогових РМ (100-108 МГц, 433 МГц) і цифрових РМ (2.4 ГГц). Принципи виявлення напівпровідникових елементів. Нелінійні радіолокатори. Металошукачі. Класифікація засобів виявлення випромінювань закладних пристроїв. Апаратура радіоконтролю. Детектори ЗУ. Апаратура придушення радіоканалів. Генератори загороджувальних і прицільних перешкод. Засоби порушення роботи закладних пристроїв. Руйнування закладних пристроїв..

13. Засоби запобігання витоку інформації через побічні та паразитні електромагнітні випромінювання та наведення. Моделі реагування на інциденти.

Паразитні перетворення. Паразитні зв'язку. Ланцюги витоку інформації. Обмеження малих амплітуд. односпрямована передача сигналів. Засоби екранування електромагнітних полів. Моделі реагування на інциденти та їх обробка.

Рекомендована література

1. Іванченко С.О., Гавриленко О.В., Липський О.А., Шевцов А.С. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації. Навчальний посібник. – К.: ІСЗЗІ НТУУ «КПІ», 2016. – 104 с.
2. Пількевич І.А., Лобанчикова Н.М.,. Молодецька К.В.Захист інформації в автоматизованих системах управління: посібник. – Житомир: Вид-во ЖДУ ім. І. Франка, 2015. – 226 с.
3. Бурячок В.Л., Толубко В.Б., Хорошко В. О., Толюпа С.В. Інформаційна і кібербезпека: соціотехнічний аспект: Підручник. – К.: ДУТ, 2015. – 288 с.
4. Толюпа С.В., Дружинін В.А., Бурячок В.Л., Наконечний В.С., Лазаренко С.В. Електроматеріали. Пасивні елементи засобів радіозв'язку та захисту інформації. Навчальний посібник. – К.: ДУТ, 2015. – 193 с
5. Бурячок В.Л., Гулак Г.М., Толубко В.Б. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби: Підручник. – К.: ДУТ, 2015. – 449 с.

2.4 Системи та технології кібербезпеки

1. Центр моніторингу та управління безпекою (SOC).
2. Елементи центру моніторингу та управління безпекою. SOC
3. Люди в SOC. Процес в SOC. Технології в SOC
4. Корпоративний SOC і послуги з управління інформаційною безпекою.
5. Захист і аналіз кінцевих пристроїв. Загрози для кінцевих пристроїв. Безпека кінцевих пристроїв.
6. Захист від шкідливого ПЗ на рівні хоста.
7. Захист від шкідливого ПЗ на рівні мережі.
8. Міжмережеві екрани на рівні хоста. Виявлення вторгнень на основі хоста. Функціонування HIDS.
9. Поверхні вразливі до атак. Формування чорного і білого списків додатків
10. Виявлення аномалій мережі. Перевірка мережі на уразливості.
11. Загальна система оцінки вразливостей (Common Vulnerability Scoring System, CVSS).
12. База вразливостей CVE.
13. Стандарт безпеки даних індустрії платіжних карт (PCI DSS).
14. Системи управління безпекою. Управління ризиками.
15. Контроль вразливостей. Управління ресурсами.
16. Корпоративне управління виправленнями.
17. Методи управління виправленнями.
18. Моніторинг безпеки. Syslog і NTP, DNS

19. Технології перетворення мережевих адрес (NAT) і перетворення адрес портів (PAT)

20. Шифрування, інкапсуляція і тунеллювання.

21. Однорангові мережі та Tor.

22. Інструмент моніторингу командного рядка tcpdump, NetFlow.

23. Моніторинг і контроль роботи додатків. Журнали фільтрації вмісту.

24. IDS та IPS нового покоління.

25. Джерела даних про безпеку. Повне перехоплення пакетів. Журнали хоста. Системний журнал. Журнали серверів.

26. Аналіз даних вторгнень. Security Onion. Інструменти виявлення для збору даних попереджень.

27. Детермінований аналіз і імовірнісний аналіз. Скорочення даних. Нормалізація даних.

28. Робота в Sguil. Обробка подій в Sguil.

29. Процес цифрової технічної експертизи. Типи доказів. Порядок збору доказів.

30. Облік зберігання речових доказів. Цілісність і збереження даних. Атрибути атак.

31. Реагування на інциденти і їх обробка.

32. Розвідувальна атака. Створення зброї. Доставка зброї.

33. Застосування експлойтів.

34. Ромбовидна модель і ланцюг кібервбивства.

35. Комп'ютерні групи реагування на надзвичайні ситуації (CERT)

36. Життєвий цикл реагування на інциденти NIST.

37. Етапи виявлення та аналізу інцидентів.

38. Стримування, усунення та відновлення.

39. Дії після інциденту. Збір і зберігання даних про інцидент

40. Вимоги до звітності та обмін інформацією.

Рекомендована література

1. CCNA Cybersecurity Operations. https://www.netacad.com/courses/security/ccna-cybersecurity-operations

2. Santos, Omar, Joseph Muniz, and Stefano De Crescenzo. *CCNA Cyber Ops SECFND# 210-250 Official Cert Guide*. Cisco Press, 2017.

3. Dulaney, Emmett, and Chuck Easttom. *CompTIA Security+ Study Guide: Exam SY0-501*. John Wiley & Sons, 2017.

4. Gregg, Michael. *Certified Ethical Hacker (CEH) Version 9 Cert Guide*. Pearson IT Certification, 2017.

5. Santos, Omar, and John Stuppi. *CCNA Security 210-260 Official Cert Guide: CCNA Sec 210-260 OCG*. Cisco Press, 2015.