**КИЇВСЬКИЙ УНІВЕРСИТЕТ ІМЕНІ БОРИСА ГРІНЧЕНКА**

ЗАТВЕРДЖЕНО
Приймальною комісією
Протокол № 5 від 29. 03. 2021 року
Голова Приймальної комісії

Віктор ОГНЕВ'ЮК

# Програма
# фахового вступного випробування зі спеціальності

| | |
|---|---|
| **Освітній рівень:** | **другий (магістерський)** |
| **Спеціальність:** | **125 Кібербезпека** |
| **Освітня програма:** | **Безпека інформаційних і комунікаційних с** |
| **На основі:** | **освітнього ступеня бакалавр, магістр, освітньо-кваліфікаційного рівня спеціаліст** |

ПОГОДЖЕНО

Проректор з науково-методичної та начальної роботи

Олексій ЖИЛЬЦОВ

РОЗГЛЯНУТО І ЗАТВЕРДЖЕНО
на засіданні кафедри інформаційної та кібернетичної безпеки Факультету інформаційних технологій та управління
протокол № 2 від 06 лютого 2021 р
Завідувач кафедри

Володимир БУРЯЧОК

Київ – 2021

# 1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

Програма розроблена кафедрою інформаційної та кібернетичної безпеки Київського університету імені Бориса Грінченка на основі навчальних програм профільних дисциплін ступеня вищої освіти – бакалавр: теоретичні основи захищених інформаційних технологій, прикладна криптологія, методи та засоби захисту інформаційно-комунікаційних систем, проектування комплексних систем захисту інформації, управління інформаційною безпекою інформаційно-комунікаційних систем.

Вступне фахове випробування проводиться у формі комп'ютерного тестування, що здійснюється протягом 80 хвилин, яке дозволить встановити рівень підготовки абітурієнта та його потенціал і можливості для навчання на спеціальності 125 «Кібербезпека».

# 2. ЗМІСТ ПРОГРАМИ ФАХОВОГО ВСТУПНОГО ВИПРОБУВАННЯ

## 2.1. Теоретичні основи захищених інформаційних технологій

**Основні парадигми формування захищених інформаційних технологій.** Основні поняття гарантовано захищених інформаційних технологій. Основи формування гарантовано захищених інформаційних технологій. Основи розроблення гарантованих систем захисту.

**Загальні моделі опису процесів захисту інформації в комп'ютерних системах.** Суб'єктно-об'єктна модель опису комп'ютерної системи. Автоматна суб'єктно-об'єктна модель опису комп'ютерної системи. Використання суб'єктно-об'єктної моделі для опису базових операції в комп'ютерній системі. Підходи до формування моделі загроз. Підходи до формування моделі порушника. Підходи та моделі опису цінності інформації: базові поняття; адитивна модель цінності інформації; порядкова шкала цінностей; модель решітки цінностей; MLS решітка. Підходи та моделі оцінки збитків автоматизованої системи та ризику її функціонування.

**Основи теорії захищених систем**. Політики управління доступом. Моделі опису політики безпеки. Моделі забезпечення конфіденційності. Моделі забезпечення цілісності. Моделі забезпечення доступності. Приклади моделювання питань безпеки в обчислювальних системах. Основи синтезу моделей безпеки.

**Забезпечення гарантій виконання вимог політик безпеки.** Загальні поняття про розроблення програмного забезпечення захисту інформації. Технологічна безпека розроблення систем захисту. Забезпечення гарантій виконання політики безпеки на основі методу генерації ізольованих програмних середовищ.

**Стандартизовані моделі опису сучасних інформаційних технологій та методи оцінки їх ефективності**. Модель, що покладена в основу

міжнародного стандарту ISO 7498-2. Модель, що покладена в основу НД ТЗІ 2.5. Модель, що покладена в основу міжнародного стандарту ISO 15408.

**Приклади побудови сучасних захищених інформаційних технологій.** Розвиток захищених обчислювальних систем. Огляд деяких захищених обчислювальних систем. Сучасні захищені середовища та їх моделі: типові умови функціонування розподілених обчислювальних середовищ з точки зору забезпечення їх цілісності; типові захищені розподілені обчислювальні середовища.

**Література**

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

2. Грушо А.А., Тимонина Е.Е. Теоретические основы защиты информации.– М.: Изд-во агентства "Яхтсмен", 1996. – 192 с.

3. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. – М.: Горячая линия-Телеком,2000. – 452 с.

4. Теоретические основы компьютерной безопасности: Учебное пособие для вузов / П.Н.Девянин, О.О.Михальский, Д.И.Правиков и др. – М.: Радио и связь, 2000. – 192 с.

5. Бурячок В.Л. Основи формування державної системи кібернетичної безпеки: Монографія. – К.: НАУ, 2013. – 432 с.

**2.2. Прикладна криптологія**

**Основи криптології**. Предмет криптології. Роль криптологічних методів в побудові систем захисту інформації. Актуальність побудови надійних систем зв’язку. Проблеми практичної криптології. Основні терміни та визначення криптології. Загальна симетрична система секретного зв’язку К. Шеннона. Загальні типи криптоатак. Практична та теоретична стійкість. Кодування відкритого тексту. Пакування довільних даних для передачі лініями зв’язку. Приклади класичних шифрів. Поняття поля. Поле GF(2). Многочлени над полем. Кільце лишків поліномів та розширення поля GF(2. Вектори і лінійні форми. Базис лінійного простору. Лінійні перетворення та матриці над полем. Підстановки, цикли і транспозиції. Підстановочні матриці. Декремент підстановки. Анулюючий та мінімальний многочлен матриці. Мінімальний многочлен матриці відносно вектора.

**Модульна арифметика та елементарні шифри.** Лишки за модулем. Відношення порівняння. Розширений алгоритм Евкліда для чисел та многочленів. Модульна арифметика. Шифри заміни, гамування та перестановки. Рандомізація. Шифри пропорційної та поліалфавітної заміни. Методика дешифрування шифру простої заміни. Шифр Кардано та шифр подвійної перестановки.

**Порівняння з одним невідомим.** Теореми Ейлера і Ферма. Порядок числа та первісний корінь за модулем. Система лінійних порівнянь та китайська теорема про залишки. Загальний метод розв’язування лінійних

порівнянь з одним невідомим. Властивості степеневих порівнянь. Двочленні порівняння вищих степенів за простим модулем. Первісний корінь за модулем $p^a$. Дискретні логарифми (індекси).

**Асиметричні криптосистеми та основні типи шифрів**. Задачі криптології, що привели до поняття асиметричних шифрів. Поняття про односторонні функції та односторонні функції з лазівками. Криптосистема RSA, криптосистема Ель-Гамаля, протокол узгодження ключів Діффі-Хеллмана. Поняття геш-функції. Цифровий підпис на основі криптосистеми RSA та криптосистеми Ель-Гамаля. Загальне рівняння для побудови цифрового підпису типу Ель-Гамаля. Слабкі параметри в криптосистемі RSA. Проблема факторизації та проблема дискретного логарифмування. Поняття ключового потоку. Потокові шифри. Блокові шифри. Режими застосування блокових шифрів. Алгоритм ГОСТ 28147-89. Слабкі ключі. Застосування регістрів зсуву для побудови вузлів криптосхем. Дешифрування шифру періодичної двійкової гами. Період лінійної двійкової рекуренти. Загальні відомості про криптографічні параметри булевих функцій та відображень.

**Вибір параметрів криптосистеми RSA**. Квадратичні лишки. Символи Лежандра та Якобі. Тестування чисел на простоту. Тест Ферма. Основні властивості псевдопростих чисел. Числа Кармайкла. Тест Соловея-Штрассена. Тест Рабіна-Міллера. Метод Гордона побудови сильно простих чисел. Алгоритм здобуття квадратного кореня в простому полі. Імовірнісне шифрування.

**Методи автентифікації інформації.** Геш-функції, що побудовані на однокрокових стискуючих функціях. Алгоритм HMAC. Застосування ГОСТ 28147-89 для генерації ПВЧ. Алгоритм MD-5. Геш-функція SHA-1. Стандарт DSS. Система S-keys. Модифікований протокол Фіата-Шаміра та схема ідентифікації Шнорра.

**Управління ключами**. Життєвий цикл ключів. Поняття про ключову систему. Протоколи транспортування та узгодження ключів. Перетворення ключів. Криптоалгоритм RC4. Формування ключів. Алгоритм DES в режимі ECB.

**Цифровий підпис на еліптичних кривих**. Еліптичні криві над скінченним полем. Нерівність Хассе. Проективні координати та операції в групі $E_n$ точок на еліптичній кривій. Схема цифрового підпису на основі циклічної підгрупи простого порядку групи $E_n$. Скінченні поля та параметри ЦП на еліптичних кривих, що використовуються в ДСТУ 4145-2002. Схема цифрового підпису стандарту ДСТУ 4145-2002.

**Сучасні системи криптографічного захисту інформації**. Прикладні аспекти сучасних методів криптографічного захисту інформації. Протокол Kerberos. Перетворення паролів у ключі. Режим PCBC алгоритму DES. Служба автентифікації X.509 v.3. Автентифікація (схема ЦП) в пакеті PGP. Загальна схема та основні перетворення криптоалгоритму AES.

**Література**

1. Богуш В.М., Мухачов В.А. Криптографічні застосування елементарної теорії чисел. Навчальний посібник. – Київ: ДУІКТ, 2006.
2. Вербицький О.В. Вступ до криптології. – Лв.: ВНТЛ, 1998. – 247 с.
3. Виноградов И. М. Основы теории чисел. —9-е изд., перераб. —М.: Наука, 1981.
4. ГОСТ 28147-89. Система обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. - М.: Изд-во стандартов, 1989. - 26 с.
5. Мухачев В.А., Хорошко В.А. Методы практической криптографии. К.: ООО „ПолиграфКонсалтинг” , 2004. –215 с.
6. Кузьминов Т.В. Криптографические методы защиты информации. Новосибирск, „Наука”, Сибирское предприятие РАН 1998. – 185 с.
7. Столингс В. Основы защиты сетей. Приложения и стандарты. - М.: Издательский дом „Вільямс”, 2002. – 432с.
8. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Изд-во ТРИУМФ,2002. – 816 с.
9. Черемушкин А.В. Лекции по арифметическим алгоритмам в криптографии. – М.: МЦНМО, 2002.

### 2.3. Методи та засоби захисту інформаційно-комунікаційних систем

**Основні положення системи технічного захисту інформації в комп'ютерних системах.** Постановка проблеми комплексного забезпечення інформаційної безпеки інформаційних та комунікаційних систем та мереж. Вразливості інформаційно-комунікаційних систем та мереж (ІКСМ) та причини їх виникнення. Основні принципи розробки комплексів засобів (КЗЗ) ІТСМ як розподілених середовищ. Нормативна база. Концепція ієрархічної декомпозиції. Поняття про політику та послуги безпеки, механізми захисту, засоби та комплекси засобів захисту. Рівні градації доступу до інформації. Література [1,2, 4, 5].

**Механізми та засоби захисту операційних систем.** Загрози операційним системам. Загальні підходи захисту від атак з метою відмови в обслуговуванні та від атак з метою отримання несанкціонованого доступу до інформації. Забезпечення цілісності даних. Розмежування прав користувачів. Механізми ідентифікації та авторизації. Шифрування даних. Використання механізмів та засобів резервування даних. Файлові системи. Особливості різноманітних файлових систем. Література [1,2,10].

**Механізми та засоби захисту операційних систем сімейства Microsoft Windows.** Особливості моделі захисту операційних систем сімейства Microsoft Windows. Штатні механізми та засоби захисту. Методика використання засобів захисту. Локальні користувачі та групи користувачів. Управління обліковими записами та профілями користувачів. Групова політика безпеки. Шаблони безпеки. Типи файлових систем. Призначення прав доступу до файлів та папок. Передача прав володіння. Використання шифруючої файлової системи. Управління сертифікатами користувачів. Резервування файлів та папок. Аудит операційної системи. Література [1,2,10,17].

**Механізми та засоби захисту систем керування базами даних.** Причини, види, основні методи порушення конфіденційності в системах керування базами даних (СКБД). Багаторівневі реляційні СКБД. Методи захисту СКБД. Особливості керування доступом. Підтримка логічної цілісності, транзакції функціонування, синхронізація в розподілених СКБД. Забезпечення безпеки багаторівневих реляційних СКБД. Особливості застосування криптографічних методів. Спільне застосування засобів ідентифікації й автентифікації, вбудованих у СКБД і в ОС. Кластерна організація серверів баз даних. Особливості реалізації механізмів захисту офісних СКБД. Література [1,5].

**Концепція системи безпеки системи керування базами даних сімейства MS SQL Server.** Призначення, традиційна сфера використання та загальнопоширені загрози СКБД сімейства MS SQL Server. Загальна характеристика системи захисту. Порядок інсталяції та першочергової настройки. Основні компоненти програмного комплексу MS SQL Server. Загальна характеристика системи автентифікації користувачів. Шифрування даних. Управління користувачами бази даних. Призначення та зміна прав користувачів. Методика реєстрації та видалення користувачів. Визначення прав доступу до об'єктів бази даних. Система привілеїв. Поняття "ролі". Використання "ролей" для керування правами користувачів. Використання графічного інтерфейсу та операторів Transact-SQL. Література [1,2,10,18].

**Методика підвищення ефективності захисту та аудит системи керування базами даних сімейства MS SQL Server.** Поняття представлень, процедур що зберігаються і тригерів в СКБД сімейства MS SQL Server. Методика використання представлень, процедур що зберігаються і тригерів для забезпечення безпеки даних. Поняття резервного копіювання та відновлення бази даних. Типи резервних копій. Методика резервного копіювання. Моделі відновлення баз даних. Методика відновлення бази даних. Поняття аудиту баз даних. Відслідковування активності користувачів, використання журналу помилок. Використання графічного інтерфейсу та операторів Transact-SQL. Література [1,2,10,18].

**Механізми та засоби захисту від шкідливих програмних засобів.** Руйнуючі програмні засоби. Програми з потенційно шкідливим впливом та їх властивості. Нормативна та законодавча база в галузі захисту від шкідливих програмних засобів. Основні класи руйнуючих програм. Віруси та „трояни", визначення та класифікація. Засоби розповсюдження. Деструктивні властивості. Модель вірусу та модель „трояна". Передумови діагностики вірусів та „троянів" на основі аналізу програмного коду та на основі аналізу подій в операційній системі. Методи та засоби контролю та протидії вірусам та „троянам". Література [1,3,5].

**Загальна характеристика комп'ютерних вірусів.** Історична довідка. Визначення комп'ютерного Вірусу. Основні властивості. Класифікація вірусів. Деструктивні можливості. Особливості файлових, мережених, загрузочних та макровірусів. Стелс та поліморфні віруси. Шляхи розповсюдження вірусів. Використання електронної пошти та офісних

документів для розповсюдження вірусів. Макровіруси в додатках Microsoft Office. Використання макросів типу AutoOpen при створенні макровірусів. Програмний код заготовки макровірусу Microsoft Office. Особливості вірусів, що пристосовані для розповсюдження за допомогою змінних носіїв інформації (Flash-пам'ять та компакт-диски). Література [1,3,5,14].

**Методи та засоби боротьби з комп'ютерними вірусами.** Профілактика зараження вірусами. Використання засобів операційної системи для протидії вірусам. Протидія розповсюдженню вірусів з змінних носіїв інформації (Flash-пам'ять та компакт-диски). Правила використання файлів, отриманих по електронній пошті. Критерії оцінки якості антивірусних програмних комплексів. Сигнатурні методи визначення вірусів. Визначення вірусів за допомогою аналізу подій. Переваги та недоліки евристичних аналізаторів. Антивірусні монітори та сканери. Порівняльна характеристика розповсюджених та ліцензованих антивірусних програм. Принципи налагодження антивірусних засобів. Навести приклад. Література [1,3,5].

**Методи та засоби боротьби з програмами кейлогерами.** Призначення програм кейлогерів. Принципи використання кейлогерів. Інтернет ресурси в яких представлені кейлогери. Інсталяція та настройка визначеного кейлогера. Визначення програм антикейлогерів. Принципи їх функціонування. Пошук кейлогерів за допомогою аналізу сигнатури. Інтернет ресурси з програмами антикейлогерами. Інсталяція та настройка визначеного антикейлогера. Література [1,5].

**Загальні положення захисту розподілених обчислювальних середовищ та мереж передачі даних.** Загальні положення про інформаційну безпеку розподілених обчислювальних середовищ та мереж передачі даних. Особливості моделі загроз. Формування розподіленої ДВБ та її властивості. Основні типи засобів забезпечення інформаційної безпеки в розподілених обчислювальних середовищах та мережах. Безпека вузлів комутації: загальні положення про інформаційну безпеку вузлів комутації; критерії захищеності програмно-керованих АТС. Особливості забезпечення захисту ком'ютерних систем сполучених з глобальною мережею Інтернет. Типи та класифікація загроз, відповідно популярним сервісам. Вразливості протоколів Інтернет. Особливості загрози типу „відмова в обслуговувані". Характеристика інструментальних засобів захисту. Політика безпеки при використанні ресурсів мережі Інтернет. Література [1,4,9,17].

**Мета та задачі використання мережевих екранів.** Призначення мережених екранів. Характеристика стеку протоколів TCP/IP. Принципи та передумови використання. Основні функції. Історія розвитку. Класифікація. Особливості апаратних та програмних реалізацій. Недоліки та переваги різних типів мережевих екранів. Політика безпеки мережених екранів. Недоліки використання. Навести приклад настройки мережевого екрану. Література [4,9,10].

**Мета та задачі використання приватних віртуальних мереж.** Основи технології віртуальних приватних мереж (ВПМ). Визначення ВПМ та засоби їх реалізації. Принципи побудови та класифікації ВПМ. Моделі порушника,

загроз та обмеження ВПМ. Основи реалізації ВПМ. Побудова ВПМ на інших рівнях моделі ВВС. Протокол SSL. Стандарти IPSec. Інфраструктура ВПМ. Навести приклад розгортання ВПМ на основі операційної системи Microsoft Windows XP. Література [4,9, 7].

**Технологія захисту від DOS та DDOS атак на комп'ютерні мережі.** Загальна характеристика протоколу TCP/IP. Етапи та схема встановлення TCP з'єднання. Поняття DOS та DDOS атак. Мета проведення атаки. Методологія реалізації DOS та DDOS атак. Сигналізація про здійснення DOS та DDOS атак. Захист за допомогою оптимізації настройок сервера. Захист за допомогою мережевих екранів. Література [1,4].

**Парольний захист об'єктів комп'ютерних мереж.** Призначення парольного захисту. Схеми реалізації. Парольний захист операційної системи, Web-ресурсів, програмних додатків та офісних документів. Принципова схема атаки з метою зламу парольного захисту . Використання „дірок" в програмному забезпеченні парольного захисту. Використання документованих можливостей для реалізації атаки. Методи підбору паролю. Класичні схеми захисту від атак з метою зламу паролю. Література [1, 5].

**Захист електронної пошти.** Типові загрози для електронної пошти: несанкціонований витік інформації, проникнення вірусів та троянів, засмічення поштового ящика. Методика захисту від типових загроз. Особливості шифрування даних. Типові прийоми захисту від запуску вірусів та троянів. Розповсюджені методи захисту від засмічення поштового ящику (захист від спаму) − білого, сірого та чорного списків, ключових фраз, байєсовської фільтрації. Недоліки та переваги. Програмні додатки захисту електронної пошти. Література [1, 5, 13].

**Захист Web-серверу Apache.** Вітчизняна нормативна база в галузі захисту Web-серверу. Нормативні критерії захищеності Web-серверу. Відповідність Apache проектним та експлуатаційним вимогам. Оцінка захищеності Apache від атаки на відмову в обслуговуванні. Параметри захисту Apache. Рекомендований порядок інсталяції та попередньої настройки. Розмежування прав користувачів. Базова та цифрова авторизація. Використання бібліотеки OpenSSL Використання додаткових модулів безпеки. Захищеність серверних технологій. Література [7,16, 19].

**Захист Web-серверу IIS**. Вітчизняна нормативна база в галузі захисту Web-серверу. Нормативні критерії захищеності Web-серверу. Відповідність IIS проектним та експлуатаційним вимогам. Оцінка захищеності IIS від атаки на відмову в обслуговуванні. Захищеність серверних технологій. Параметри захисту IIS. Інтеграція IIS з системою безпеки Windows. Розмежування прав користувачів. Особливості ідентифікації та авторизації користувачів. Захищеність серверних технологій. Література [7,16,17].

**Перспективні напрями розвитку комплексів засобів захисту інформації в розподілених середовищах.** Адаптивні комплекси засобів захисту інформації; системи виявлення вторгнень; системи керування захищеністю; комплекси засобів захисту інформації мобільних програмних систем. Основи систем аналізу вразливостей. Визначення та принципи

класифікації. Програмне забезпечення систем аналізу вразливостей. Основи систем виявлення вторгнень. Визначення та принципи класифікації. Програмне забезпечення систем виявлення вторгнень. Використання в системах виявлення вразливостей та в системах виявлення вторгнень засобів штучного інтелекту. Системи активного захисту. Література [13,1,5].

**Безпека мобільних пристроїв.** Характеристика специфічних загроз для мобільних пристроїв. Обмеження програмного забезпечення, що використовується в мобільних пристроях: віртуальної машини Java та Framework. Особливості програмних засобів захисту мобільних пристроїв. Інструментальні засоби захисту мобільних пристроїв провідних виробників. Література [1, 5,12, 13].

**Література**


1. Щеглов А.Ю. Защита компьютерной информации от НСД. Санкт-Петербург: Наука и техника – 2004, 384 с.
2. Джон Вэк и Лиза Карнахан Введение в межсетевые экраны
3. WordBasic и макровирусы (kiev-security.da.ru)
4. Медведовский АТАКА ЧЕРЕЗ INTERNET
5. Соколов А.,Степанюк О. Защита от компьютерного терроризма. СПб.: Арлит, 2002 496 с.
6. НД ТЗІ 1.1-003-99. Термінологія в галузі захисту ...
7. НД ТЗІ 2.5-010-03. Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу.
8. ДСТУ 3396.2-97. Терміни та визначення
9. Персональный брандмауэр «Outpost Firewall». Руководство пользователя
10. Таненбаум Компьютерные сети. – СПб.: Питер, 2003. – 992 с.
11. Терейковский И.А. Парольная защита офисного электронного документооборота / И. А. Терейковский // Вісник ДУІКТ. − 2006. − Т. 4, № 2 − С. 109−115.
12. Терейковський И. А. Применение семантического анализа содержимого электронных писем в системах распознавания спама / И. А. Терейковский // Захист інформації. – 2006. − № 4. – С. 49−60.
13. Хорошко В. А. Использование искусственных нейронных сетей в задачах распознавания атак на компьютерные системы / В. А. Хорошко, И. А. Терейковский // Захист інформації. − 2006. − №3. − С. 57−65.
14. Терейковський І. Використання можливостей Microsoft Access при створенні Веб - орієнтованих вірусів.
15. Терейковский И. А. Безопасность программного обеспечения, созданного с использованием семейства технологий COM, DCOM, COM+ / И. А. Терейковский // Захист інформації. − 2006. − № 1. − С. 55−67.
16. Терейковський І. А. Захищеність Web-серверів Apache та IIS / І. А. Терейковський // Проблеми програмування. − 2005. − № 2. − С. 42−51.
17. Андреев А.Г. и др. Microsoft Windows XP. /Под общей ред. А.Н. Чекмарева. – СПб.: БХВ-Петербург, 2003. – 640 с.

18. Марк Шпеник М., Следж Ор. Руководство администратора баз данных MS SQL Server.

19. Хокинс С. Администрирование Web-сервера Apache и руководство по электронной коммерции. : Пер. с англ. М. : Издательский дом “Вильямс”, 2001. – 336 с.

20. Бурячок В.Л., Толубко В.Б., Хорошко В. О., Толюпа С.В. Інформаційна і кібербезпека: соціотехнічний аспект: Підручник. – К.: ДУТ, 2015. – 288 с.

21. 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 технічного захисту інформації

**Технічні канали витоку інформації.** Особливості витоку інформації. Характеристики технічних каналів витоку інформації. Класифікація каналів витоку інформації.

**Акустичні канали витоку інформації**. Структура акустичного каналу витоку інформації. Характеристики акустичного каналу витоку інформації. Класифікація аудіоканалу витоку інформації.

**Радіоелектронні канали витоку інформації**. Структура радіоелектронного каналу витоку інформації. Характеристики радіоелектронних каналів витоку інформації. Класифікація радіоканалів витоку інформації.

**Оптичні канали витоку інформації**. Структура оптичного каналу витоку інформації. Характеристики оптичного каналу витоку інформації. Класифікація оптичних каналів витоку інформації.

**Закладні пристрої**. Структура закладних пристроїв. Класифікація закладних пристроїв. Закладні пристрої з передачею по радіоканалу. Закладні пристрої з передачею по провідним каналам.

**Засоби перехоплення інформації за допомогою мікрофонів**. Структурна схема акустичного приймача. Класифікація та види мікрофонів.

**Засоби перехоплення інформації за допомогою диктофонів.** Аналогові диктофони. Цифрові диктофони.

**Оптичні засоби перехоплення інформації**. Структурна схема засобу перехоплення в оптичному діапазоні. Об’єктиви. Візуально-оптичні прилади. Фото- і кіноапарати. Засоби телевізійного спостереження. Відеомагнітофони. Прилади нічного бачення. Тепловізори.

**Перехоплення інформації в засобах зв’язку**. Структура типового комплексу перехоплення. Антени. Радіоприймачі

**Виявлення закладних пристроїв**. Демаскуючі ознаки закладних пристроїв. Класифікація засобів виявлення в локалізації закладних пристроїв. Індикатори поля. Апаратура радіоконтролю. Принципи контролю телефонних ліній та кіл електроживлення. Засоби придушення сигналів закладних пристроїв. Апаратура нелінійної локації. Виявники пустот, металодетектори

та рентгенівські апарати. Способи та методи контролю приміщень на відсутність закладних пристроїв.

**Програмно-апаратні пристрої захисту інформації**. Захист від несанкціонованого доступу. Захист від копіювання. Захист від вірусів.

**Основні способи захисту інформації технічними засобами.** Класифікація методів захисту інформації. Охорона джерел інформації. Приховування інформації: інформаційне приховування, енергетичне приховування.

**Апаратура захисту ліній зв'язку**. Методи і засоби захисту телефонних ліній і апаратів. Засоби контролю телефонних ліній та апаратів. Технічні засоби виявлення телефонних радіоретрансляторів. Криптографічні методи та засоби захисту мовної інформації.

**Засоби створення акустичних маскуючих завад**. Генератори шуму в акустичному діапазоні. Пристрої віброакустичного захисту. Пристрої ультразвукового захисту приміщень.

**Засоби створення електромагнітних маскуючих завад**. Засоби просторового зашумлення. Засоби лінійного зашумлення. Засоби створення маскуючих завад в комунікаційних мережах. Засоби створення маскуючи завад в мережах електроживлення. Багатофункціональні засоби захисту.

**Література**

1. Ленков С.В., Перегудов Д.А. Хорошко В.А. Методы и средства защиты информации. Том 1. Несанкционированное получение информации. К.: Издательство Арий, 2008.

2. Ленков С.В., Перегудов Д.А. Хорошко В.А. Методы и средства защиты информации. Том 2. Информационная безопасность. К.: Издательство Арий, 2008.

3. Торокин А.А. Основы инженерно-технической защиты информации. – М.: Издательство «Ось-89», 1998, - 336 с.

4. Хорошко В.А., Чекатков А.А. Методы и средства защиты информации. К.: Изд. Юниор, 2003. – 504с.

### 2.5. Комплексні системи захисту інформації

**Загальні положення та вимоги щодо організації робіт із захисту інформації та порядку створення комплексної системи захисту інформації в ІКС**. Поняття комплексної системи захисту інформації (КСЗІ) в ІКС. Основні нормативно-правові акти щодо організації робіт із захисту інформації та порядку створення КСЗІ в ІКС. Єдність порядку створення КСЗІ на всіх етапах життєвого циклу ІКС. Процес створення КСЗІ як здійснення комплексу взаємоузгоджених заходів, спрямованих на розроблення і впровадження інформаційної технології, яка забезпечує обробку інформації в ІКС згідно з вимогами, встановленими нормативно-правовими актами та нормативних документів (НД) у сфері захисту інформації. Порядок створення КСЗІ в ІКС

як сукупність впорядкованих у часі, взаємопов'язаних, об'єднаних в окремі етапи робіт, виконання яких необхідне й достатнє для КСЗІ, що створюється.

**Основні засоби та заходи, що входять до складу КСЗІ.** КСЗІ як заходи та засоби, які реалізують способи, методи, механізми захисту інформації від: витоку технічними каналами, до яких відносяться: канали побічних електромагнітних випромінювань і наведень, акустоелектричні та інші канали; несанкціонованих дій та несанкціонованого доступу до інформації, що можуть здійснюватися шляхом підключення до апаратури та ліній зв'язку, маскування під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав'язування хибної інформації, застосування закладних пристроїв чи програм, використання комп'ютерних вірусів та ін; спеціального впливу на інформацію, який може здійснюватися шляхом формування полів і сигналів з метою порушення цілісності інформації або руйнування системи захисту. Вплив властивостей оброблюваної інформації, класу автоматизованої системи та умов експлуатації ІКС на склад, структуру та вимоги до КСЗІ. Забезпечення режиму секретності, протидії технічним розвідкам та організаційні заходи щодо охорони інформації з обмеженим доступом у процесі проектування, розроблення, виготовлення, експлуатації ІКС. Створення комплексів захисту інформації КЗЗ від витоку технічними каналами. Модульний принцип побудови КСЗІ інтегрованої в ІКС.

**Порядок створення, завдання, функції, структура та повноваження служби захисту інформації щодо організації робіт зі створення КСЗІ в ІКС.** Загальну положення про службу захисту інформації (СЗІ). Завдання СЗІ. Функції СЗІ: під час створення КСЗІ; під час експлуатації КСЗІ; з організації навчання персоналу з питань забезпечення захисту інформації. Повноваження та відповідальність СЗІ: права СЗІ; обов'язки СЗІ; відповідальність СЗІ; взаємодія СЗІ з іншими підрозділами та зовнішніми організаціями; штатний розклад та структура СЗІ. Організація робіт служби захисту інформації. Фінансування СЗІ.

**Обґрунтування необхідності створення КСЗІ.** Підстава для визначення необхідності створенні КСЗІ. Вихідні дані для обґрунтування необхідності створення КСЗІ. Прийняття рішення про необхідність створення КСЗІ.

**Обстеження середовищ функціонування ІКС.** Обстеження обчислювальної системи ІКС. Обстеження інформаційного середовища. Обстеження фізичного середовища. Обстеження середовища користувачів. Акт обстеження. План захисту інформації в ІКС. Перелік об'єктів захисту. Потенційні загрози для інформації, модель загроз та модель порушника.

**Формування завдання на створення КСЗІ**. Завдання захисту інформації в ІКС, мета створення КСЗІ, варіант вирішення задач захисту, основні напрями забезпечення захисту. Аналіз ризиків (вивчення моделі загроз і моделі порушника, можливих наслідків від реалізації потенційних загроз, величини можливих збитків та ін.) і визначення переліку суттєвих загроз. Визначення загальної структури та складу КСЗІ, вимоги до можливих заходів, методів та засобів захисту інформації, допустимі обмеження щодо застосування певних заходів і засобів захисту (обмеження щодо використання

засобів активного захисту від витоку інформації каналами ПЕМВН за рахунок використання засобів ЕОТ в захищеному виконанні тощо), інші обмеження щодо середовищ функціонування ІКС, обмеження щодо використання ресурсів ІКС для реалізації задач захисту, припустимі витрати на створення КСЗІ, умови створення, введення в дію і функціонування КСЗІ (окремих її підсистем, компонентів), загальні вимоги до співвідношення та меж застосування в ІКС (окремих її підсистемах, компонентах) організаційних, інженерно-технічних, технічних, криптографічних та інших заходів захисту інформації, що ввійдуть до складу КСЗІ. Оформлення звіту про виконання робіт цієї стадії та оформлення заявки на розробку КСЗІ.

**Розробка політики безпеки інформації в ІКС.** Вивчення об'єкта**,** на якому створюється КСЗІ, проведення науково-дослідних робіт. Вибір варіанту КСЗІ. Оформлення політики безпеки.

**Розробка технічного завдання на створення КСЗІ**. Призначення та основний зміст технічного завдання (ТЗ). Варіанти оформлення ТЗ на КСЗІ. Особливості ТЗ на КСЗІ для інтегрованих ІКС, які будуються за модульним принципом.

**Розробка проекту КСЗІ.** Порядок розробки проекту КСЗІ. Ескізний проект КСЗІ. Технічний проект КСЗІ. Робочий проект КСЗІ.

**Введення КСЗІ в дію та оцінка захищеності інформації в ІКС.** Підготовка організаційної структури та розробка розпорядчих документів, що регламентують діяльність із забезпечення захисту інформації в ІКС. Навчання користувачів. Комплексування КСЗІ. Будівельно-монтажні роботи. Пусконалагоджувальні роботи. Попередні випробування. Дослідна експлуатація. Державна експертиза КСЗІ.

**Супроводження КСЗІ.** Порядок виконання робіт з організаційного забезпечення функціонування КСЗІ та управління засобами захисту інформації відповідно до плану захисту та експлуатаційної документації на компоненти на компоненти КСЗІ, гарантійному та післягарантійному технічному обслуговуванню засобів захисту інформації.

**Література**

1. Домарєв В.В., Скворцов С.О. Організація захисту інформації на об'єктах державної та підприємницької діяльності. Навч. посібник. – К.: Вид-во Європ. Ун-ту, 2006. – 102 с.

2. Доценко С.М., Шпак. В.Ф. Комплексная безопасность объекта: от теории к практике. С.-Петербург: ООО «Издательство Полигон», - 2000.

3. Гришина Н.В. Организация комплексной защиты информации. – М.: Гелиос АРВ, 2007. – 256 с.

4. ДСТУ 3396.1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт.

5. ДБН А.2.2-2-96 Проектування. Технічний захист інформації. Загальні вимоги до організації проектування та проектної документації для будівництва.

6. ДБН 2.2-3-2004 Склад, порядок розроблення, погодження та затвердження проектної документації для будівництва.

7. Закон України “Про захист інформації в інформаційно-телекомунікаційних системах” (в редакції Закону N 2594-IV від 31.05.2005).

8. Ленков С.В., Перегудов Д.А. Хорошко В.А. Методы и средства защиты информации. Том 1. Несанкционированное получение информации. К.: Издательство Арий, 2008.

9. Ленков С.В., Перегудов Д.А. Хорошко В.А. Методы и средства защиты информации. Том 2. Информационная безопасность. К.: Издательство Арий, 2008.

10. ГОСТ 34.201 - 89 Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем.

11. ГОСТ 34.601 - 90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания.

12. ГОСТ 34.602 - 89 Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы.

13. Завгородний В.И. Комплексная защита информации в компьютерных системах: Учебное пособие. – М.: Логос; ПБОЮЛ Н.А. Егоров, 2001. – 264 с.

14. Комплекс стандартов Единая система программной документации (ЕСПД)

15. Комплекс стандартов Единая система конструкторской документации (ЕСКД)

16. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 № 22.

17. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі. Затверджено наказом ДСТСЗІ СБ України від 04.12.2000 № 53.

18. НД ТЗІ 2.1-001-2001 Створення комплексів технічного захисту інформації. Атестація комплексів. Основні положення. Затверджено наказом ДСТСЗІ СБ України від 09.02.2001 № 2.

19. НД ТЗІ 1.1-005-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.

20. НД ТЗІ 2.1-002-07 Захист інформації на об’єктах інформаційної діяльності. Випробування комплексу технічного захисту інформації. Основні положення.

21. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 № 22.

22. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від

несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 № 22.

23. НД ТЗІ 2.5-008-2002 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2. Затверджено наказом ДСТСЗІ СБ України від 13.12.2002 № 84.

24. НД ТЗІ 2.5-010-2003 Вимоги до захисту інформації WEB - сторінки від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 02.04.2003 № 33.

25. НД ТЗІ 3.1-001-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні роботи

26. НД ТЗІ 3.3-001-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації.

27. НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 20.12.2000 № 60.

28. НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 № 22.

29. НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. Затверджено наказом ДСТСЗІ СБ України від 08.11.2005 № 125.

30. РД 50 - 34.698 - 90 Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Требования к содержанию документов.

31. Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітних випромінювань і наводок. (ТР ЕОТ-95). Затверджені наказом ДСТЗІ від 09.06.1995 № 25.

32. Тимчасові рекомендації з технічного захисту інформації від витоку каналами побічних електромагнітних випромінювань і наводок. (ТР ТЗІ-ПЕМВН-95). Затверджені наказом Державної служби України з питань технічного захисту інформації від 09.06.95 № 25.

33. Положення про державну експертизу в сфері технічного захисту інформації. Затверджене наказом ДСТСЗІ СБ України від 29.12.1999 №62 і зареєстроване в Міністерстві юстиції України 24.01.2000 за №40/4261.

34. Положення про дозвільний порядок проведення робіт з технічного захисту інформації для власних потреб. Затверджене наказом ДСТСЗІ СБ України від 23.02.2002 № 9 і зареєстроване в Міністерстві юстиції України 13.03.2002 за № 245/6533.

35. Торокин А.А. Основы инженерно-технической защиты информации. – М.: Издательство «Ось-89», 1998, - 336 с.

36. Бурячок В.Л., Грищук Р.В., Хорошко В. О. Політика інформаційної безпеки: Підручник. – К.: ДУТ, 2014. – 222 с.

## 2.6. Управління інформаційною безпекою в інформаційно-комунікаційних системах

**Передумови та основні напрямки розвитку менеджменту у сфері інформаційної безпеки.** Мета, завдання, передумови та напрямки організаційної і управлінської роботи у сфері інформаційної безпеки. Діяльність міжнародних організацій у сфері інформаційної безпеки. Діяльність спеціалізованих міжнародних організацій у сфері інформаційної безпеки. Управління інформаційною безпекою на рівні потужних постачальників інформаційних систем.

**Управління інформаційною безпекою на державному рівні.** Передумови розвитку державного управління у сфері інформаційної безпеки. Загальна методологія і структура організаційного забезпечення інформаційної безпеки на рівні держав. Управління інформаційною безпекою на державному рівні на прикладі України.

**Основи управління інформаційною безпекою на рівні підприємства.** Передумови розвитку управління у сфері інформаційної безпеки на рівні підприємств. Загальна структура управлінської роботи із забезпечення інформаційної безпеки на підприємстві.

**Нормативно-правові основи побудови системи управління інформаційною безпекою інформаційно-комунікаційної системи підприємства.** Стандарти управління інформаційною безпекою. Itil. Cobit 4.1. Стандарти серії ISO/IEC 27000. Стандарти серії ДСТУ ISO/IEC 13335. НД ТЗІ. Інші стандарти.

**Управління інформаційною безпекою на основі стандартів серії ISO/IEC 27000.** Загальна характеристика стандартів серії ISO/IEC 27000. Огляд стандарту ISO/IEC 27001. Галузь застосування стандарту ISO/IEC 27001. Структура стандарту ISO/IEC 27001. Модель системи управління інформаційною безпекою. Вимоги стандарту і способи їх реалізації.

**Формування політики інформаційної безпеки на підприємстві.** Структура політики інформаційної безпеки на підприємстві та процес її розробки.

**Служба інформаційної безпеки на підприємстві**. Організаційна структура служби інформаційної безпеки. Робота з персоналом підприємства.

**Основні види правил управління інформаційною безпекою відповідно до стандарту ISO/IEC 27002 та їх документаційне оформлення**. Правила фізичної безпеки. Правила автентифікації і безпеки мережі. Правила безпечної роботи в Інтернеті. Правила безпеки електронної пошти. Правила антивірусного захисту. Правила застосування шифрування. Правила розробки програмного забезпечення. Типові документи, засновані на вимогах стандарту ISO/IEC 27002.

Аналіз і управління **ризиками інформаційної безпеки**. Створення реєстру ризиків. Ідентифікація загроз і уразливостей. Оцінка ризиків. Управління ризиками.

**Аудит інформаційної безпеки на підприємстві**. Поняття аудиту безпеки. Стандарт COBIT. Практика проведення аудиту безпеки. Етапи проведення аудита безпеки: ініціювання процедури аудита; збирання інформації аудита; аналіз даних аудита; вироблення рекомендацій; підготовка аудиторського звіту.

**Організація реагування на надзвичайні події (інциденти)**. Поняття інциденту інформаційної безпеки. Виявлення інцидентів. Реагування на інцидент: аналіз інциденту, розслідування інциденту, звіт про інцидент. Попередження інцидентів. Усунення наслідків інцидентів.

**Розробка та впровадження системи управління інформаційною безпекою.** Етапи розробки і впровадження системи управління ІБ. Організаційні аспекти впровадження системи управління інформаційною безпекою. Особливості побудови системи управління інформаційною безпекою на основі стандартів серії ISO/IEC 27000. Сертифікація системи управління інформаційною безпекою.

**Використання програмних засобів для підтримки управління безпекою.** Програмна підтримка роботи з політикою безпеки. Програмна підтримка аналізу ризиків. Програмні комплекси для створення системи управління ІБ.

**Надання послуг у сфері інформаційної безпеки.** Передумови розвитку ринку послуг забезпечення інформаційної безпеки та його структура. Особливості деяких видів послуг. Страхування інформаційних ризиків. Основи методології страхування інформаційних ресурсів. Ринок страхових послуг.

**Література**


1. Анисимов А.А. Менеджмент в сфере информационной безопасности М.: БИНОМ. 2009.
2. Бармен Скотт. Разработка правил информационной безопасности М.: Издательский дом “Вильямс”, 2002.
3. Богуш В.М., Кудін А.М. Моніторинг і аудит систем інформаційної безпеки. К.: ДУІКТ, 2006, - 340 с.
4. Гринберг А.С. и др. Защита информационных ресурсов государственного управления. М.: ЮНИТИ-ДАНА, 2003.
5. ГСТУ СУІБ 1.0/ISO/IEC 27001:2010. Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги. К.: НБУ, 2010.
6. ГСТУ СУІБ 2.0/ISO/IEC 27002:2010. Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Звід правил для управління інформаційною безпекою. К.: НБУ, 2010.

7. ДСТУ ISO/IEC TR 13335-1:2003. Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 1. Концепції та моделі безпеки. К.: Держспоживстандарт України, 2005.
8. ДСТУ ISO/IEC TR 13335-2:2003. Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 2. Керування та планування безпеки ІТ. К.: Держспоживстандарт України, 2005.
9. ДСТУ ISO/IEC TR 13335-3:2003. Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 3. Методи керування захистом ІТ. К.: Держспоживстандарт України, 2005.
10. ДСТУ ISO/IEC TR 13335-4:2005. Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 4. Настанови з керування безпекою інформаційних технологій. К.: Держспоживстандарт України, 2005.
11. ДСТУ ISO/IEC TR 13335-5:2005. Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 5. Настанови з керування мережною безпекою. К.: Держспоживстандарт України, 2005.
12. Курило А.П., Зефиров С.Л., Голованов В.Б. и др.. Аудит информационной безопасности. – М.: Издательская группа “БЦД-пресс”, 2006. – 304 с.
13. Петренко С.А., Курбатов В.А. Политики информационной безопасности. – М.: Компания АйТи, 2006. – 400 с.
14. Петренко С.А., Симонов С.А. Управление информационными рисками. Экономически оправданная безопасность. – М.: Компания АйТи, 2004. - 384 с.

## 3. ПИТАННЯ ДЛЯ ПІДГОТОВКИ ДО ВИПРОБУВАННЯ

### 3.1. Теоретичні основи захищених інформаційних технологій

1. Основні поняття гарантовано захищених інформаційних технологій.
2. Формування гарантовано захищених інформаційних технологій
3. Розробка гарантованих систем захисту.
4. Моделі опису функціонування комп’ютерних систем.
5. Основні моделі середовища функціонування комп’ютерної системи.
6. Політики управління доступом.
7. Моделі опису політики безпеки.
8. Моделі забезпечення конфіденційності.
9. Моделі забезпечення цілісності.
10. Моделі забезпечення доступності.
11. Синтез моделей безпеки.
12. Основні положення щодо розробки програмного забезпечення захисту інформації.
13. Технологічна безпека розроблення систем захисту
14. Забезпечення гарантій виконання політики безпеки на основі методу генерації ізольованих програмних середовищ.

15. Модель безпеки, що покладена в основу міжнародного стандарту ISO 7498-2.

16. Модель безпеки, що покладена в основу НД ТЗІ 2.5. Загальні положення моделі. Функціональні критерії.

17. Модель безпеки, що покладена в основу НД ТЗІ 2.5. Критерії гарантій безпеки. Функціональні профілі захищеності.

18. Модель безпеки, що покладена в основу міжнародного стандарту ISO 15408. Основні положення загальних критеріїв безпеки інформаційних технологій. Функціональні вимоги до засобів захисту.

19. Модель безпеки, що покладена в основу міжнародного стандарту ISO 15408. Вимоги гарантій засобів захисту. Рівні гарантій безпеки.

20. Сучасні захищені операційні системи.

### 3.2. Прикладна криптологія

1. Порядки чисел за модулем. Доведення теорем Ейлера та Ферма.
2. Цифровий підпис Ель-Гамаля.
3. Лінійна двійкова рекурентна послідовність у якості гами. Генератор псевдовипадкових чисел ANSI X9.17.
4. Тестування чисел на простоту. Імовірнісні та детерміновані тести. Тест на основі малої теореми Ферма.
5. Тест Соловея-Штрассена перевірки чисел на простоту.
6. Тест Рабіна-Міллера перевірки чисел на простоту.
7. Загальні відомості про іноземні криптозасоби.
8. Визначення геш-функції. Побудова геш-функції, виходячи з блочного шифра.
9. Ключові системи потокових шифрів. Життєвий цикл ключів.
10. Груповий закон на невиродженій еліптичній кривій в афінних координатах. Аналог протоколу Діффі-Хеллмана а групі точок на еліптичній кривій.
11. Актуальність проблеми надійності діючих систем криптографічного захисту інформації.
12. Загальна симетрична система секретного зв’язку за К. Шенноном. Основні терміни та визначення криптології.
13. Проблема розподілу ключів та її вирішення за допомогою односпрямованих функцій з лазівками. Асиметричні криптосистеми.
14. Визначення та приклади основних та елементарних типів шифрів.
15. Алгоритм ГОСТ 28147-89 в режимі простої заміни та режимі гамування із зворотним зв’язком.
16. Алгоритм розв’язування порівняння першого степеня з одним невідомим. Формулювання китайської теореми про залишки.
17. Двочленні квадратичні порівняння. Властивості символу Лежандра.
18. Двочленні квадратичні порівняння. Властивості символу Якобі.
19. Побудова криптосистеми RSA. Ідея цифрового підпису.
20. Змішані криптосистеми. Протокол Діффі-Хеллмана узгодження ключів.

### 3.3.Методи та засоби захисту інформаційних і комунікаційних систем

1. Основні положення системи технічного захисту інформації в комп'ютерних системах.
2. Механізми та засоби захисту операційних систем.
3. Механізми та засоби захисту операційних систем сімейства Microsoft Windows.
4. Механізми та засоби захисту систем керування базами даних.
5. Концепція системи безпеки системи керування базами даних сімейства MS SQL Server.
6. Методика підвищення ефективності захисту та аудит системи керування базами даних сімейства MS SQL Server.
7. Механізми та засоби захисту від шкідливих програмних засобів.
8. Загальна характеристика комп’ютерних вірусів.
9. Методи та засоби боротьби з комп’ютерними вірусами.
10. Методи та засоби боротьби з програмами кейлогерами.
11. Загальні положення захисту розподілених обчислювальних середовищ та мереж передачі даних.
12. Мета та задачі використання мережевих екранів.
13. Мета та задачі використання приватних віртуальних мереж.
14. Технологія захисту від DOS та DDOS атак на комп’ютерні мережі.
15. Парольний захист об’єктів комп’ютерних мереж.
16. Захист електронної пошти.
17. Захист Web-серверу Apache.
18. Захист Web-серверу IIS.
19. Перспективні напрями розвитку комплексів засобів захисту інформації в розподілених середовищах.
20. Безпека мобільних пристроїв.

### 3.4. Системи технічного захисту інформації

1. Технічні канали витоку інформації. Загальна характеристика.
2. Акустичні канали витоку інформації.
3. Радіоелектронні канали витоку інформації.
4. Оптичні канали витоку інформації..
5. Закладні пристрої.
6. Засоби перехоплення інформації за допомогою мікрофонів.
7. Засоби перехоплення інформації за допомогою диктофонів.
8. Оптичні засоби перехоплення інформації.
9. Перехоплення інформації в засобах зв’язку.
10. Виявлення закладних пристроїв.
11. Програмно-апаратні пристрої захисту інформації.
12. Основні способи захисту інформації технічними засобами.
13. Апаратура захисту ліній зв’язку.
14. Засоби створення акустичних маскуючих завад.

15. Засоби створення електромагнітних маскуючих завад.

### 3.5 Комплексні системи захисту інформації

1. Загальні положення та вимоги щодо організації робіт із захисту інформації та порядку створення комплексної системи захисту інформації в ІКС.
2. Основні засоби та заходи, що входять до складу КСЗІ.
3. Порядок створення, завдання, функції, структура та повноваження служби захисту інформації щодо організації робіт зі створення КСЗІ в ІКС.
4. Обґрунтування необхідності створення КСЗІ.
5. Обстеження середовищ функціонування ІКС.
6. Формування завдання на створення КСЗІ.
7. Розробка політики безпеки інформації в ІКС.
8. Розробка технічного завдання на створення КСЗІ.
9. Розробка проекту КСЗІ.
10. Введення КСЗІ в дію та оцінка захищеності інформації в ІКС.
11. Супроводження КСЗІ.

### 3.6. Управління інформаційною безпекою в інформаційно-комунікаційних системах

1. Передумови та основні напрямки розвитку менеджменту у сфері інформаційної безпеки.
2. Управління інформаційною безпекою на державному рівні.
3. Основи управління інформаційною безпекою на рівні підприємства.
4. Нормативно-правові основи побудови системи управління інформаційною безпекою інформаційно-комунікаційної системи підприємства.
5. Управління ІБ на основі стандартів серії ISO/IEC 27000.
6. Формування політики інформаційної безпеки на підприємстві.
7. Служба інформаційної безпеки на підприємстві.
8. Основні види правил управління інформаційною безпекою відповідно до стандарту ISO/IEC 27002 та їх документаційне оформлення.
9. Аналіз і управління ризиками інформаційної безпеки.
10. Аудит інформаційної безпеки на підприємстві.
11. Організація реагування на надзвичайні події (інциденти).
12. Розробка та впровадження системи управління інформаційною безпекою.
13. Використання програмних засобів для підтримки управління безпекою.
14. Надання послуг у сфері інформаційної безпеки.

## Критерії оцінювання знань вступника

| Кількість балів (max - 200) | Критерії |
|---|---|
| **180 – 200** | Виставляється за глибокі знання навчального матеріалу, що міститься в основних і додаткових рекомендованих джерелах; вміння аналізувати явища, які вивчаються, у їхньому взаємозв'язку і розвитку, чітко і лаконічно; логічно і послідовно відповідати на поставлені запитання; вміння застосовувати теоретичні положення під час розв'язання практичних задач. |
| **160 – 179** | Виставляється за ґрунтовні знання навчального матеріалу, аргументовані відповіді на поставлені запитання; вміння застосовувати теоретичні положення під час розв'язування практичних задач. |
| **140 – 159** | Виставляється за міцні знання навчального матеріалу, аргументовані відповіді на поставлені запитання, які, однак, містять певні неточності; вміння застосовувати теоретичні положення під час розв'язання практичних задач. |
| **120 – 139** | Виставляється за посередні знання навчального матеріалу, мало аргументовані відповіді, слабке застосування теоретичних положень при розв’язанні практичних задач. |
| **100 – 119** | Виставляється за слабкі знання навчального матеріалу, неточні або мало аргументовані відповіді, з порушенням послідовності його викладання, за слабке застосування теоретичних положень при розв’язанні практичних задач. |
| **1 – 99** | Виставляється за незнання значної частини навчального матеріалу, істотні помилки у відповідях на запитання, невміння орієнтуватися під час розв'язання практичних задач, незнання основних фундаментальних положень. |

## 4.ПЕРЕЛІК ДОВІДКОВИХ МАТЕРІАЛІВ НА ВИПРОБУВАННЯ

1. Богуш В.М., Кривуца В.Г., Кудін А.М. Інформаційна безпека: термінологічний навчальний довідник. – К.: ООО “Д.В.К.” 2004. – 508 с.

2. ГОСТ 28147-89. Система обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. - М.: Изд-во стандартов, 1989. - 26 с.

3. ГСТУ СУІБ 1.0/ISO/IEC 27001:2010. Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги. К.: НБУ, 2010.

4. ГСТУ СУІБ 2.0/ISO/IEC 27002:2010. Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Звід правил для управління інформаційною безпекою. К.: НБУ, 2010.

5. ДСТУ ISO/IEC TR 13335-1:2003. Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 1. Концепції та моделі безпеки. К.: Держспоживстандарт України, 2005.
6. ДСТУ ISO/IEC TR 13335-2:2003. Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 2. Керування та планування безпеки ІТ. К.: Держспоживстандарт України, 2005.
7. ДСТУ ISO/IEC TR 13335-3:2003. Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 3. Методи керування захистом ІТ. К.: Держспоживстандарт України, 2005.
8. ДСТУ ISO/IEC TR 13335-4:2005. Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 4. Настанови з керування безпекою інформаційних технологій. К.: Держспоживстандарт України, 2005.
9. ДСТУ ISO/IEC TR 13335-5:2005. Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 5. Настанови з керування мережною безпекою. К.: Держспоживстандарт України, 2005.
10. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення. Чинний від 01.07.1997 р. - К.: Держстандарт України, 1997. - 7 с.
11. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт. Чинний від 01.07.1997 р. - К.: Держстандарт України, 1997. - 7 с.
12. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.
13. НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.
14. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.
15. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.
16. НД ТЗІ 3.7-001-99. Методичні вказівки щодо розроблення технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі.
17. НД ТЗІ 3.7-005-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. Затверджено наказом ДСТЗІ СБ України від 08.11.2005 р. №125.
18. НД ТЗІ 2.5-010-03. Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу.
19. Термінологічний довідник з питань технічного захисту інформації / Коженевський С.Р., Кузнецов Г.В., Хорошко В.О., Чирков Д.В. / За ред. проф. В.О. Хорошка. – К.: ДУІКТ, 2007. – 365 с.