МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД

“УЖГОРОДСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ”

ФІЗИЧНИЙ ФАКУЛЬТЕТ

Кафедра твердотільної електроніки та інформаційної безпеки

«ЗАТВЕРДЖУЮ»
Декан фізичного факультету
_____/Лазур В.Ю./
«__» _____ 2022 року

Робоча програма навчальної дисципліни
ПРОГРАМА ДО ДЕРЖАВНОГО ІСПИТУ

рівень вищої освіти **другий (магістерський)**

галузь знань **12 Інформаційні технології**
(шифр і назва)

Спеціальність **125 Кібербезпека**
(шифр і назва)

освітньо- професійна програма
Безпека інформаційних і комунікаційних систем
(шифр і назва)

спеціалізація

статус дисципліни **обов’язкова**
(обов’язкова/за вибором)

Мова навчання **українська**

Ужгород 2022

Робоча програма навчальної дисципліни «**ПРОГРАМА ДО ДЕРЖАВНОГО ІСПИТУ**» для здобувачів вищої освіти галузі знань **12 Інформаційні технології** спеціальності **125 Кібербезпека** освітньої програми «**Безпека інформаційних і комунікаційних систем».**

Розробник: к. фіз.-мат. н., доц. Січка М.Ю.

Робочу програму розглянуто та затверджено на засіданні кафедри твердотільної електроніки та інформаційної безпеки
протокол № 7 від «28» 04 2022 р.

Завідувач кафедри _____ Різак В.М.

Схвалено науково-методичною комісією фізичного факультету
протокол № 10 від «29» 04 2022 р.
Голова науково-методичної комісії _____ Карбованець М. І.

ПРОГРАМА

До державного іспиту за напрямом підготовки 8.125- Кібербезпека. Безпека інформаційних і комунікаційних систем

Технології створення та застосування систем захисту інформаційно-комунікаційних систем

1. Інформація та її властивості. Загальні поняття про інформаційні системи та технології. Основні функції інформаційних систем.
2. Нейронні мережі прямого та зворотного поширення як інформаційно-комунікаційні системи.
3. Нейронні мережі з алгоритмом самоорганізації Хебба як інформаційно-комунікаційні системи.
4. Нейронні мережі з алгоритмом самоорганізації Кохонена як інформаційно-комунікаційні системи.
5. Будова нейрона як інформаційно-комунікаційні система.
6. Штучний нейрон як інформаційно-комунікаційні система та його будова.
7. Біометрія та інформаційне поле людини.
8. Структуровані біологічні системи (вода, рідини) та їх інформаційне поле.
9. Символьне розпізнавання за допомогою одношарового перцептрона та алгоритму Хебба.
10. Композиція нейронних мереж з алгоритмами Хебба та прямого поширення в системах символьного кодування.
11. Фрактальні інформаційні структури як інформаційно-комунікаційні системи.
12. Фрактал Серпінського та визначеня його розмірності.
13. Інформаційні коміркові перколяційні системи та їх застосування в інформаційно-комунікаційних технологіях.
14. Клітинкові інформаційні структури, що еволюціонують з формуванням однорідних, стаціонарних або періодичних структур.
15. Атрактори (точкові та циклічний атрактори) та відповідні інформаційні структури як інформаційно-комунікаційні системи.
16. Атрактори (тор, дивний атрактор) та відповідні інформаційні структури як інформаційно-комунікаційні системи.
17. Біфуркаційна діаграма та формування інформаційно-комунікаційні системи.Нелінійні інформаційні моделі при формуванні інформаційно-комунікаційної системи.
18. Системи організації інформаційних ресурсів, багаторівневі схеми збереження документів з різним інтервалом доступу.
19. Візуальне програмування та особливості його використання в інформаційно-комунікаційних системах. Технологія VCL, Ole, DLL.
20. Електронний цифровий підпис при формуванні інформаційно-комунікаційної системи.
21. Grid–технології, кластаризація та об'єднання ресурсів. Їх застосування та модифікація в БІКС
22. Синергетика та інформаційно-комунікаційні системи. Сигентропія та формування інформаційно-комунікаційної системи. Ентропія закритих та відкритих інформаційних систем.
23. Алгоритмічна складність Чепмена-Колмогорова для інформаційно-комунікаційних систем.
24. Інформаційні технології та сфери їх застосування. Етапи розвитку інформаційних технологій.

Технологія адміністрування та експлуатації захищених інформаційно-телекомунікаційнихсистем

1. Модель загроз для операційної системи
2. Типова архітектура комплексу засобів захисту операційних систем
3. Порівняльна характеристика підходів до побудови захищених систем

4. Критерії оцінювання захищених комп'ютерних систем Міністерства оборони США (TCSEC)
5. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу (НД ТЗІ)
6. Стандарт ISO 15408: основні документи, структура профілю захисту і завдання з безпеки
7. Стандарт ISO 15408: структура стандарту, основні документи, структура вимог
8. Компоненти КЗЗ ОС Windows. Взаємодія компонентів і БД системи безпеки
9. Підсистема розмежування доступу ОС Windows. Суб'єкти і об'єкти доступу . Реалізація дискреційного керування доступом
10. Алгоритми з'ясування прав доступу в ОС Windows
11. Реалізація підсистеми ідентифікації й автентифікації в ОС Windows
12. ITU-T, рекомендації X.800. Основні сервіси і механізми безпеки в мережах
13. Проблеми протоколу IP і його реалізацій з точки зору безпеки інформації. Основні атаки на IP
14. Проблеми протоколів Telnet і FTP. Уразливості. Методи захисту.
15. Безпека системи електронної пошти.
16. Безпека служби WWW: вразливості клієнтського ПЗ. Підвищення ступеня захищеності клієнтського ПЗ.
17. Безпека служби WWW: вразливості серверного ПЗ. Приклади атак.
18. Віртуальні приватні мережі (VPN). Сервіси віртуальних приватних мереж. Типи віртуальних приватних мереж
19. VPN віддаленого доступу. Протоколи PPTP і L2TP
20. VPN сеансового рівня: функції посередництва, протоколи 38.Засоби виявлення атак і протидії атакам

Технологія організації інфраструктури відкритих ключів

1. Порівняльний аналіз національної та міжнародної нормативно – правової бази в частині ІВК (ЕЦП) та напрями удосконалення і розвитку національної бази.
2. Електронні довірчі послуги. Класифікація та формати сертифікатів відкритих ключів
3. Генерування та використання асиметричних пар ключів ЕЦП у прикладних системах
4. Життєві цикли особистих ключів та сертифікатів відкритих ключів.
5. Обслуговування сертифікатів відкритих ключів. Аналіз та оцінка механізмів відкликання сертифікатів відкритих ключів
6. Вимоги до архітектури ІВК (ЕЦП), побудова та аналіз шляхів сертифікації
7. Валідація шляхів сертифікації при наданні електронних довірчих послуг
8. Стандартизація у галузі ІВК та надання електронних довірчих послуг
9. Класифікація протоколів ІВК, особливості, застосування та аналіз
10. Основні існуючі та перспективні положення політик сертифікації.
11. Проблеми теорії та практики надання електронних довірчих послуг
12. Дослідження стандартизованих криптографічних протоколів ЕЦП по критеріям стійкості та складності
13. Дослідження механізмів створення запиту та виготовлення сертифікатів відкритих ключів національної системи ЕЦП
14. Дослідження механізмів генерування асиметричних пар ключів на робочих станціях та на відокремлених пунктах реєстрації
15. Аналіз стану та дослідження механізмів забезпечення криптографічної живучості в ІВК (системі ЕЦП)
16. Дослідження бізнес процесів акредитованого центру сертифікації ключів. Регламент акредитованого центру сертифікатів ключів (ЦСК) та його застосування
17. Формати сертифікатів відкритих ключів та списків відкликаних сертифікатів.
18. Дослідження активності ЦСК та вимоги до пропускної здатності ЦСК
19. Аналіз процесів та процедур розгортання ЦСК для застосування в комерційних чи банківських системах
20. Основні додатки застосування системи ЕЦП (ІВК) та оцінка їх ефективності.

Теорія ризиків

1. Формування ринку цінних паперів. Ринок державних цінних паперів.
2. Біржова торгівля. Фондові біржі. Біржі і біржова торгівля.
3. Фундаментальний аналіз фондового ринку.
4. Технічний аналіз фондового ринку.
5. Система інститутів та інфраструктура фондового ринку
6. Функції, операції та ризики фондового ринку
7. Прийоми і фігури технічного аналізу фондового ринку.
8. Фондовий ринок: сила руху; осцилятори; інтерпретація моменту і швидкості зміни.
9. Крайні положення ринку. Індекс відносної сили (RSI). Тимчасові періоди для RSI. Зміна значень. Розбіжності RSI.
10. Спільне використання індикаторів ринку: японські свічки, бари, лінії.
11. Міжнародні фінансові системи. Основи поняття фінансового ринку. Учасники міжнародного фінансового ринку.
12. Трендові моделі. Правила побудови та аналізу. Підтвердження
13. Класичні фігури технічного аналізу.
14. Загальні риси і протиріччя трендових моделей. Термін життя тренда і його життєвий цикл. Правила побудови та їх види. Правила аналізу
15. Побудова і аналіз двох середніх на одному графіку і комбінації пар середніх. Канали зміни цін.
16. Побудова і аналіз MACD (метод конвергенції-дивергенції-сходження-розходження). Інші трендові індикатори
17. Побудова і аналіз індикатора "спрямованого зміни" (Directional Movement - +/- DM). Побудова і аналіз середнього індикатора вірогідною спрямованості (ADX).
18. Осцилятори. Правила аналізу. Аналіз показників обсягу. Виявлення моменту укладення угоди.
19. Витоки динамічного технічного аналізу. Аналіз бажання ринку, його напрямку та сили.
20. Теорія циклів. Криволінійна модель динаміки ціни Белла ("Bell curve model").
21. Хвильова теорія Елліотта. Індикатори фондового ринку. Індекс трейдера.
22. Індикатори фондового ринку. Механічні торгові системи. Система "трьох екранів".
23. Управління ризиками . Основні принципи системи управління ризиками

Математичні методи моделювання і оптимізації процесів

1. Моделювання процесів. Методи моделювання процесів
2. Оптимізація процесів та систем. Опукла оптимізація. Основні методи оптимізації
3. Поняття про задачі оптимізації. Основні типи розв'язку задач оптимізації
4. Класифікація задач математичного програмування
5. Задача лінійного програмування.
6. Графічний метод для розв'язання задач лінійного програмування
7. Симплексний метод розв'язування задач лінійного програмування
8. Задачі дробово-лінійного програмування. Методи розв'язування дробово-лінійної задач.
9. Розв'язування дробово-лінійної задачі зведенням до задачі лінійного програмування
10. Задачі нелінійного програмування. Методи розвязку ЗНЛП
11. Метод множників Лагранжа. Необхідні умови існування сідлової точки.
12. Квадратичне моделювання. Постановка задачі квадратичного моделювання
13. Умови Теореми Куна—Такера для задач квадратичного програмування
14. Моделювання випадкових величин із заданим законом розподілу.
15. Моделювання генераторів випадкових та псевдовипадкових чисел
16. Теорія ігор. Матричні ігри
17. Динамічні процеси. Методи моделювання динамічних систем.
18. Моделювання динаміки популяцій.
19. Фрактальниї аналіз складних процесів.
20. Синергетичне моделювання і управління складними процесами.

21. Застосування теорії хаосу в імітаційному моделюваня

Інтелектуальна власність

1. Виникнення, становлення і розвиток поняття інтелектуальної власності.
2. Поняття права інтелектуальної власності. Співвідношення права власності і права інтелектуальної власності.
3. Авторське право. Поняття і види результатів творчості, що охороняються авторським правом. Об'єкти авторського права.
4. Суб'єкти авторських відносин. Суб'єктивне авторське право, його зміст і межі: особисті немайнові права авторів; майнові права автора та іншої особи, що має авторське право; вільне використання творів; право на авторську винагороду;
5. Суміжні права, суб'єкти суміжних прав. Захист авторського права і суміжних прав.
6. Поняття промислової власності. Об'єкти промислової власності.
7. Винахід. Корисна модель. Об'єкти винаходу і корисної моделі. Умови надання правової охорони винаходу (корисній моделі). Умови надання правової охорони винаходу (корисній моделі). Патент. Промисловий зразок. Суб'єкти права на винаходи, корисні моделі і промислові зразки.
8. Право на одержання патенту, право авторства.
9. Порядок оформлення та подання заявки на винахід. Корисну модель і промисловий зразок. Вимога єдності винаходу. Загальні вимоги до змісту документів заявки. Склад заявки. Опис винаходу (корисної моделі). Формула винаходу (корисної моделі). Вимоги до ілюстративних матеріалів. Реферат та вимоги до нього. Документи, що додаються до заявки.
10. Процедура подання заявки на одержання патенту України на винахід.Подання заявки. Пріоритет винаходу.
11. Експертиза заявки на винахід за формальними ознаками.
12. Експертиза заявки на винахід по суті. Оскарження рішення за заявкою. Публікація відомостей про винахід.
13. Тимчасова правова охорона. Процедура видачі патенту на винахід (корисну модель).
14. Винаходи, що становлять державну таємницю.
15. Сплата збору за дії, пов'язані з охороною прав на винаходи (корисні моделі).
16. Припинення дії патенту та визнання його недійсним.
17. Патентування винаходу (корисної моделі) в іноземних державах. Патентування винаходу в іноземних державах за процедурою договору про патентну кооперацію (PCT). Процедура одержання європейського патенту. Процедура ЕВРО-PCT. Патентування винаходів за процедурою євразійської патентної конвенції.
18. Реалізація патентних прав. Передача права на використання. Особисті немайнові права. Майнові права субєктів права на винахід, корисні моделі і промислові зразки. Обмеження прав власника патенту.
19. Методи комерціалізації права на обєкти інтелектуальної власності.
20. Методи оцінки права на обєкти інтелектуальної власності.
21. Обовязки власника патенту. Взаємовідносини співвласників патенту.
22. Ліцензії на право користування обєктами інтелектуальної власності. Види ліцензій. Обовязкові умови та реквізити ліцензійного договору. Відкрита ліцензія. Примусове відчуження прав на винахід. Захист прав патентовласника. Авторські договори їх види.
23. Всесвітня організація інтелектуальної власності. Міжнародна охорона промислової власності. Міжнародна охорона літературної і художньої власності (авторське право).

Бездротові інформаційно-комунікаційні системи та їх проектування

1. Технологічні аспекти розвитку бездротових телекомунікаційних технологій.
2. Стандарт IEEE 802.11b: CCK-модуляція, її суть. Фізична інтерпретація автокореляції зі зміщенням. Диференціальна квадратурна модуляція (DQPSK).

3. Бездротові локальні, міські та сенсорні мережі.
4. Технології побудови глобальних мереж: IP-адреси, класи IP-адрес.
5. Стандарт IEEE 802.11a. Формування OFDM-символів. BPSK, QPSK, 16-QAM. Процедури формування вихідного сигнала.
6. Система доменних імен DNS.
7. Маршрутизація. Таблиця маршрутизації. Процес аналізу IP-адрес, який виконується з використанням таблиць маршрутизації.Три категорії маршрутизаторів. Протоколи маршрутизації.
8. Архітектура і логічна структура мережі Bluetooth. Стандарти Bluetooth і HomeRF. Порівняльні характеристики технологій Bluetooth і HomeRF. Стек протоколів Bluetooth.
9. Класифікація основних компонентів комп'ютерних мереж. Основні варіанти топології КМ.
10. Реальна, автономна, відкрита, комунікаційна, реальна остаточна, абонентська система. Рівні моделі взаємодії відкритих систем
11. Прикладний процес, середовище передавання даних, протокол, інтерфейс, стек протоколів, архітектура комп'ютерної мережі, масштаб комп'ютерної мережі, локальні, регіональні та глобальні комп'ютерні мережі, діаметр мережі, трафік
12. Протоколи стеку TCP/IP. Рівні стеку протоколів TCP/IP. Ввзаємодія прикладних процесів з використаннямпротокольного стеку TCP/IP.
13. Канал зв'язку. Сигнал. Кабельні канали зв'язку. Коаксіальний кабель, волоконно- оптичні кабелі, вита пара. Апаратура для утворення каналів зв'язку. Етапи перетворення повідомлень у сигнали і навпаки, мета перетворень.
14. Специфікація IEEE 802.15.3. Пікомережа. Надшвидкодіючі персональні мережі IEEE 802.15.3a.
15. Амплітудно-частотна та фазово-частотна характеристики фізичного середовища передавання сигналів. Категорії завад.
16. MAC-рівень стандарту IEEE 802.11.MAC-адреси. Структура байтів різних варіантів MAC-адрес.
17. Низькошвидкісні мережі стандарту IEEE 802.15.4 (ZigBee).
18. Класифікація систем передачі інформації за принципом синхронізації, за напрямками передавання.
19. Фізичний рівень стандарту IEEE 802.16-2004. Режим OFDM. Загальна тривалість OFDM символу Кодування даних на фізичному рівні в стандарті IEEE 802.16-2004. Рандомізація. Каскадний код.
20. Обладнання комп'ютерних мереж: DSL-модеми, мережні адаптери, їх характеристики
21. Методи ущільнення фізичного середовища зв'язку. Характеристики каналів зв'язку перепускна здатність, максимальна швидкість передавання даних, надійність, затримка,завадостійкість, вартість передавання даних
22. Методи кодування у каналах зв'язку: код NRZ (Non Return to Zero), код RZ (Return to Zero), Манчестерський код, код PAM5.

Методи побудови та аналізу криптосистем"

1. **Основні поняття криптоаналізу**. Терміни, визначення та основні ідеї.
2. Принцип Керкгоффса.
3. Симетричні алгоритми.
4. Криптосистеми з відкритим ключем.
5. Модель загрози Долева-Яо.
6. Основні параметри шифрів. Стійкість шифру.
7. Статистичні характеристики шифру.
8. Складність зламу шифру.
9. Складність виконання операцій шифрування та дешифрування.
10. Типи криптоаналітичних атак.

11. Шкода, завдана зламом шифру.
12. Універсальні методи та інструменти криптоаналізу. Частотний аналіз.
13. Метод повного перебору.
14. Атаки, базовані на властивостях ключів.
15. Диференціальний криптоаналіз. Лінійний криптоаналіз.
16. Атаки на криптосистеми з відкритим ключем.
17. Криптоаналіз за допомогою побічних каналів.
18. Метод Полларда.
19. Метод "зустрічі посередині".
20. Джерела відкритого тексту. Характеристики відкритих текстів.
21. Абетки відкритих текстів.
22. Повторюваність букв, біграм, n – грам (частотні характеристики тексту).
23. Стійкість та частотні характеристики біграм, триграм та чотириграм осмислених текстів.
24. Тематика відкритих текстів.
25. Внутрішня структура текстів.
26. Імовірнісні моделі відкритих текстів.
27. Посимвольна ймовірнісна модель відкритого тексту.
28. Імовірнісна модель відкритого тексту з незалежними біграмами.
29. Імовірнісна модель відкритого тексту з Марковськими залежними буквами.
30. Нестаціонарні джерела повідомлень.
31. Критерії розпізнавання осмислених відкритих текстів.
32. Надійність шифрів. Імовірнісна модель шифру.
33. Теоретико-інформаційна стійкість шифрів. Досконало стійкі шифри.
34. Шифр Вернама за модулем.
35. Деякі відомості з математичної теорії інформації.
36. Невизначеність шифру за ключем.
37. Ентропія та надлишковість мови.
38. Відстань єдиності.
39. Практична стійкість шифрів.
40. Імітостійкість шифрів.
41. Криптоаналіз класичних шифроалгоритмів. Шифри простої заміни (буквенні підстановки).
42. Криптоаналіз шифрів простої заміни.
43. Лінійна алгебра над Z_m .
44. Шифр Хілла.
45. Криптоаналіз шифру Хілла за вибраним відкритим текстом.
46. Криптоаналіз шифру Віженера.
47. Елементи криптоаналізу шифрів перестановки.
48. Міра неоднозначності відновлення відкритого тексту за криптограмою.

Стандартизація, сертифікація засобів та комплексів захисту інформації

1. Міжнародні стандарти з інформаційної безпеки.
2. «Оранжева книга»: основні положення.
3. ISO 15408-1999 “Загальні критерії оцінки безпеки інформаційних технологій»: основні положення.
4. Стандарт ISO/IES 17799-2005 «Практичні правила управління безпекою інформації»: основні положення.
5. Види послуг в галузі ТЗІ.
6. Порядок ліцензування господарської діяльності в галузі ТЗІ.
7. Порядок ліцензування господарської діяльності в галузі криптографічного захисту інформації.
8. Сертифікація засобів ТЗІ.
9. Сертифіковані технічні засоби захисту інформації.

10. Сертифіковані засоби криптографічного захисту інформації.
11. Експертиза в галузі ТЗІ. Об'єкти та суб'єкти експертизи. Форми документів.
12. Порядок проведення експертизи в галузі ТЗІ.
13. Нормативні документи, що регламентують ліцензування видів господарської діяльності в галузі ТЗІ.

Автоматизоване проектування технічних засобів захисту інформації

1. Фізичні основи утворення каналів витоку інформації
2. Методи і технічні засоби побудови технічних систем інформаційної безпеки, їх структура
3. Аналіз і особливості каналів витоку та несанкціонованого доступу до інформації в автоматизованих системах
4. Апаратна реалізація сучасних технічних методів несанкціонованого доступу до інформації
5. Сучасні технічні засоби виявлення загроз інформації
6. Розрахунок імовірності зламування на основі логічної функції системи
7. Концепція інтегрального захисту інформації
8. Комп'ютерна стеганографія як сучасний технічний та програмний засіб захисту інформації від несанкціонованого доступу
9. Загальні принципи і методи виявлення технічних каналів витоку інформації
10. Технічні засоби та технології захисту інформаційних систем від електромагнітного впливу
11. Організаційно-адміністративні засоби захисту інформації
12. Засоби і методи захисту акустичної інформації від витоку технічними каналами

Теорія розподілених інформаційних ресурсів, захист баз даних та знань

1. Аудит інформаційних систем. Захист інструментів аудиту інформаційних систем
2. Основні концепції обробки даних
3. Управління обліковими записами користувачів бази даних
4. Засоби резервного копіювання даних
5. Відновлення баз даних
6. Забезпечення цілісності та актуальності інформації в базах даних
7. Організація безпосереднього доступу до сервера СУБД
8. Доступ до різнорідних даних в Інтернет
9. Системи інтеграції неоднорідних баз даних
10. Однорідні й неоднорідні розподілені бази даних. Особливості інтеграції локальних БД в РБД
11. Проблема фільтрації інформації, що містять електронні інформаційні ресурси
12. Розподілений доступ до інформаційного середовища
13. Захист при статистичній обробці даних
14. Методи взлому веб сторінки
15. Методи захисту веб сторінки від редагування інформації
16. Загрози доступності бази даних або знань: атака на відмову в обслуговуванні
17. Хмарні технології
18. Створення власного інформаційного ресурсу
19. Аналіз існуючих та доступних хмарних сховищ
20. Захист серверів баз даних під час роботи в мережі
21. Механізми надання дезінформації засобами безпечної бази даних

Технологія адміністрування та експлуатація захищених інформаційно-комунікаційних систем

1. Постановка проблеми комплексного забезпечення інформаційної безпеки автоматизованих інформаційних систем.

2. Завдання, які вирішуються при адмініструванні інформаційних систем.
3. Мережеві та комунікаційні служби.
4. Служби аудиту та управління безпекою.
5. Служба обліку автоматизованих інформаційних систем.
6. Загальні характеристики та архітектура експертних систем.
7. Зміст інформаційного забезпечення автоматизованих систем управління.
8. Служби контролю характеристик автоматизованих інформаційних систем.
9. Архівація і відновлення даних автоматизованих інформаційних систем.
10. Загальні принципи проектування автоматизованих інформаційних систем.
11. Постановка проблеми комплексного забезпечення інформаційної безпеки автоматизованих систем.
12. Основні принципи побудови систем захисту інформації в автоматизованих інформаційних системах.
13. Комплексна систем захисту інформації.
14. Особливості проектування на сучасному рівні і синтез комплексних систем інформаційних систем.
15. Методи і методики проектування комплексних систем інформаційних систем від несанкціонованого доступу.
16. Методи і методики оцінки якості комплексних систем інформаційних систем.
17. Атестація автоматизованих систем за вимогами безпеки.
18. Особливості експлуатації комплексних систем інформаційних систем на об'єкті захисту.
19. Моделі захисту інформації в автоматизованих інформаційних систем.
20. Реалізація системи управління доступом в автоматизованих інформаційних систем.

Моніторинг та аудит інформаційно-комунікаційних систем

1. Поняття моніторингу та аудиту інформаційних систем та мета їх проведення. Зовнішній та внутрішній аудит. Цілі аудиту.
2. Методи аналізу даних при аудиті ІБ.
3. Аналіз інформаційних ризиків підприємства. Описати процес аналізу ризиків.
4. Методи оцінювання ризиків підприємства.
5. Керування інформаційними ризиками. Назвати етапи процесу керування ризиками.
6. Передумови створення стандартів ІБ.
7. Стандарт «Критерії надійності комп'ютерних систем» (Оранжева книга).
8. Гармонізовані (узгоджені) критерії оцінки безпеки інформаційних технологій європейських країн. (ITSEC).
9. Германський стандарт BSI.
10. Британський стандарт BS 7799.
11. Міжнародний стандарт ISO 17799.
12. Міжнародний стандарт ISO 15408 – «Загальні критерії»
13. Стандарт COBIT.
14. Аналіз різновидів програмних продуктів що використовуються для проведення аудиту інформаційної безпеки.
15. Система CRAMM.
16. Система Кондор.
17. Мережеві сканери.
18. Основні принципи (підходи) до проведення аудиту інформаційної безпеки.
19. Задачі і зміст робіт при проведенні аудиту ІБ.
20. Підготовка підприємства до проведення аудиту інформаційної безпеки.
21. Планування процедури аудиту ІБ.
22. Організація робіт по аудиту ІБ.
23. Алгоритм проведення аудиту безпеки підприємства.

24. Перелік даних необхідних для проведення аудиту ІБ.
25. Рекомендації по підготовці звітних документів по аудиту.
26. Економічна оцінка забезпечення Інформаційної безпеки.

Література

1. Грайворонський М. В., Новіков О. М. Безпека Інформаційно-Комунікаційних Систем. – К.: Видавнича група BHV, 2009. – 608 с.
2. Горбенко Ю.І., Горбенко І.Д. Інфраструктури відкритих ключів . Системи ЕЦП. Теорія та практика. Монографія. Харків. Форт. 2010 , 593с.
3. Інфраструктура відкритих ключів: технології, архітектура, побудова та впровадження / [О. В. Потій, А. В. Лєншин, Л. С. Сорока, В. І. Єсін і ін.]. – Дніпропетровськ: Академія митної служби України, 2011. – 202с.
4. Потій О.В., Іщенко Ю.М., Лєншин А.В. Текст лекцій з дисципліни «Побудова та розгортання інфраструктури відкритих ключів», Харків, ХНУРЕ, 2009 р.
5. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Підручник. Харків. Форт. 2013р. , 878с.
6. Горбатов В.С. Основы технологии PKI / В.С. Горбатов, О.Ю. Полянская. – М. : Горячая линия – Телеком, 2004. – 246с.
7. Стеценко І. В. Моделювання систем: навч. посіб. / І. В. Стеценко. – Черкаси : ЧДТУ, 2010. – 399 с.
8. Томашевський В. М. Моделювання систем: підручник / В. М. Томашевський. – К. : Видавнича група BHV, 2005. – 352 с.
9. Катренко А.В. Системний аналіз об'єктів та процесів комп'ютеризації: Навчальний посібник. – Львів: «Новий світ-2000», - 2003.
10. Кудрявцев Е.М. GPSS Word. Основы имитационного моделирования различных систем.- М. ДМК Пресс, 2004
11. Советов Б.Я, Яковлев С.А. Моделирование систем. М., Высшая школа, 1985г.
12. Васильков Ю. В. Компьютерные технологии вычислений в математическом моделировании: учеб. Пособие / Ю. В. Васильков, Н. Н. Василькова. – М.: Финансы и статистика, 2002. – 256 с.
13. Трусов П. В. Введение в математическое моделирование: учеб. пособие / П. В. Трусов. – М.: Логос, 2005. – 440с.
14. Алиев Т.И. Основы моделирования дискретных систем. – СПб:СПбГУ ИТМО, 2009. – 363 с.
15. Самарский А.А., Михайлов А.П. Математическое моделирование. Идеи. Методы. Примеры. – 2-е изд., исправл. – М., 2001.
16. Бирюков Р.С., Городецкий С.Ю., Григорьева С.А.,и др.. Методы оптимизации в примерах и задачах.Учебно-методическое пособие. – Нижний Новгород: Нижегородский госуниверситет, 2010. – 101 с.
17. К.Н. Мезенцев. Учебное пособие «Моделирование систем в среде AnyLogic 6.4.1».Часть 2 /Под редакцией Заслуженного деятеля науки РФ, д.т.н., профессора А.Б.Николаева. МАДИ. — М.: 2011. 103 с
18. Сайко В.Г., Казіміренко В.Я., Літвінов Ю.М. Мережі бездротового широкосмугового доступу. Навчальний посібник. – К.: ДУТ, 2015. – 196 с.
19. Широкополосные беспроводные сети передачи информации. В.Вишневский, А.Ляхов, С.Портной, И.Шахнович.М.: Горячая линия, 2005, -596 с.
20. Компютерні мережі з бездротовим доступом. В.Ф. Олійник, С.Г.Бунін та ін. – К.:Ніка-Центр, 2007. -296 с.
21. Мультисервисные сети и услуги широкополосного доступ. А.Т., Гургенидзе, В.И. Кореш В.И. Изд. Наука и Техника, Санкт Петербург, 2003,- 400 с.
22. Современные технологии беспроводной связи. И.В.Шахнович. Изд. Техносфера, 2006.- 288 с.
23. Методичні вказівки до виконання лабораторних робіт з дисципліни "Комп'ютерні мережі", для студентів напряму підготовки 6.050102 "Комп'ютерна інженерія", усіх форм навчання. Частина 1. Бездротові мережі / Укл. Г.Г. Киричек, С.Ю. Скрупський. – Запоріжжя: ЗНТУ, 2013. – 46 с.

24. Методичні вказівки до виконання лабораторних робіт з дисципліни "Проектування комп'ютерних мереж" для студентів спеціальностей 7.05010201, 8.05010201 "Комп'ютерні системи та мережі" та 7.05010203, 8.05010203 "Спеціалізовані комп'ютерні системи", усіх форм навчання.
Бездротові мережі. Частина 2 / Укл. Г.Г.Киричек, С.Ю.Скрупський. – Запоріжжя: ЗНТУ, 2015. – 50 с.
25. Кузнецов Г.В.,Фомичов В.В.,Сушко С.О.,Фомичова Л.Я. Математичні основи криптографії: Навчальний посібник, Ч. 1. — Дніпропетровськ: Нац. гірн. ун–т, 2004. – 391 с.
26. Сушко С.О.,Кузнецов Г.В.,Фомичова Л.Я., Корабльов А.В. Математичні основи криптоаналізу: Навчальний посібник. – Дніпропетровськ: Нац. гірн. ун–т, 2010. – 465 с.
27. Фомичев В.М. Дискретная математика и криптология. Курс лекций. – Москва: ДИАЛОГ–МИФИ, 2003. – 400 с.
28. Вербіцький О.В. Вступ до криптології. – Львів: Видавництво науково–технічної літератури, 1998. – 248 с.
29. Харин Ю.С.,Берник В.И.,Матвеев Г.В. Математические основы криптологии: Учебное пособие. – Минск: БГУ, 1999. – 319 с.
30. Menezes A.J.,van Oorschot P.C.,Vanstone S. Handbook of Applied Cryptography, 5th print. – CRS Press, 2001. – 816 p. (Price $ 89.95)
31. Закон України "Про наукову і науково-технічну експертизу"
32. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах"
33. Закон України "Про Державну службу спеціального зв'язку та захисту інформації України"
34. Положення про технічний захист інформації в Україні, затверджене Указом Президента України від 27 вересня 1999 року № 1229;
35. Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації, затверджене постановою Кабінету Міністрів України від 24.06.2006 № 868
36. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджені постановою Кабінету Міністрів України від 29.03.06 № 373;
37. Положення про державну експертизу в сфері технічного захисту інформації, затверджене наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 16.05.2007 № 93, зареєстрованим в Міністерстві юстиції України 16.07.2007 за № 820/14087"
38. http://www.dsszzi.gov.ua/dsszzi/control/uk/ (Офіційний сайт Державної служби спеціального зв'язку та захисту інформації України)
39. Попович Н.І. Ліцензування, атестація та сертифікація у сфері безпеки об'єктів інформаційної діяльності (методичні вказівки до вивчення курсу).- Ужгород: УжНУ, 2015. – 51 с.
40. Г.А. Бузов, С.В. Калинин, А.В. Кондратьев. Защита информации от утечки по техническим каналам: Ученое пособие. М.: «Горячая линия – Телеком», 2005., - 416 с.
41. Архипов О.Є., Луценко В.М., Худяков В.О. Захист інформації в телекомунікаційних мережах та системах зв'язку: навчально-метод. Посіб. – К.: ІВЦ "Видавництво "Політехніка", 2003. – 40 с.
42. НД ТЗІ 1.1-005-07. Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.
43. ДБН А.2.2-2-96. Державні будівельні норми України. Проектування. Технічний захист інформації. Загальні вимоги до організації проектування і проектної документації для будівництва. Київ 1996р
44. НД ТЗІ 3.1-001-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні роботи.
45. 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.
46. Чеховский С. Вопросы построения комп'ютеров, защищенных от утечки информации по каналам электромагнитного излучения.- «Правове, нормативне та метрологічне забезпечення

систем захисту інформації в Україні». Наук. тех. збірник. Київ, НТУУ «КПІ», вип.. 7, 2003 р., с.с. 194 – 198.
47. Положення про технічний захист інформації в Україні, затверджене Указом Президента України від 27.09.99 № 1229/99;
48. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення.
49. 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. Затвердж. наказом ДСТСЗІ СБ України від 20.12.2000 р. № 60.
50. НД ТЗІ 2.3-002-2001 Технічний захист мовної інформації в симетричних абонентських аналогових телефонних лініях. Засоби пасивного приховування мовної інформації. Нелінійні атенюатори та загороджувальні фільтри. Методика випробувань.Затверджено наказом ДСТСЗІ СБ України від 06.04.2001р. №11.
51. Пасічник В.В. та ін. Глобальні інформаційні системи та технології: моделі ефективного аналізу, опрацювання та захисту даних. Монографія / В.В. Пасічник, П. І. Жежнич, Р. Б. Кравець, А. М. Пелещишин, Д. О. Тарасов. Львів: Видавництво Львівської політехніки, 2006. 348 с. ISBN: 966-553-578-1.
52. Ревунков Г.И., Самохвалов Э.Н., Чистов В.В. Базы и банки данных и знаний: Учеб. для вузов / Под ред. Четверикова В.Н. – М.: Высш. шк., 1992. – 367 с.
53. Мейер Д. Теория реляционных баз данных: Пер. с англ. – М.: Мир, 1987. – 608 с.
54. Исаченко, Александр Николаевич. Модели данных и системы управления базами данных : пособие для студ. / А.Н. Исаченко, С.П. Бондаренко. - Минск : БГУ, 2007. - 220 с.
55. Когаловский М.Р. Энциклопедия технологий баз данных. - М.: Финансы и статистика, 2002. - 800 с.
56. В.И. Аверченков Аудит информационной безопасности, Учебное пособие для вузов [электронный ресурс] 2-е изд., стереотип. – М. : ФЛИНТА, 2011. – 269 с. ISBN 978-5-9765-1256-6
57. С.А. Михайлов, Ю.С. Шевцов Нові функції аудиту та моніторингу у забезпеченні кібербезпеки підприємств Інформатика та математичні методи в моделюванні 2011 Том 1, №3 243-247
58. Менеджмент інформаційної безпеки: навчальний посібник / Т.М. Тардаскіна, В.Г. Кононович –Одеса: ОНАЗ ім. О.С. Попова, 2009. –265 с.
59. Шевцов Ю.С., Кононович В.Г., Кільдішев В.Й. Модель спільного використання системи виявлення і обробки атак із системою постійного аудита інформаційної безпеки // Вісник Східноукраїнського національного університету ім.В. Даля. – 2010. – № 9(151), ч.1. С. 52-58.
60. ITU-T Recommendation ISO/IEC 18043. Information technology –Security techniques –Selection, deployment and operations of intrusion detection systems. –Geneva, 2006. –46 p. – Режим доступу: http://www.itu.int/net/home/index.aspx
61. Чунарьова А. Реалізація середовища аудиту та моніторингу сучасних інформаційно-комунікаційних систем та мереж Ukrainian Scientific Journal of information Securiti, 2013, vol.19, ussue 2 h.88-93
62. Чунарьова А.В. Підсистеми моніторингу функціонування корпоративних мереж / А.В. Чунарьова, О.К. Юдін // Захист інформаційно-комунікаційних систем: науково-практична конференція, 26-28 травня 2009, Київ. – К.: НАУ, 2009. – С. 59-60.

Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 2.5-004-99. — [Чинний від 1999.04.28]. — К. : ДСТСЗІ СБУ, 1999. № 22. (Нормативний документ системи технічного захисту інформації).

62. Юдін О.К, Чунарьова А.В.Сучасні методи аудиту інформаційно-комунікаційних систем та мереж *Національний авіаційний університет (НАУ), Україна* Современные информационные технологии.Информационная безопасность.