МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

Кафедра кібербезпеки та DATA-технологій, факультет №6

МЕТОДИЧНІ МАТЕРІАЛИ

ДО ПРАКТИЧНИХ ЗАНЯТЬ

з навчальної дисципліни «Комплексні системи захисту інформації: проектування, впровадження, супровід»

вибіркового компонент освітньої програми
першого (бакалаврського) рівня вищої освіти

125 «Кібербезпека» («Безпека інформаційних та комунікаційних систем»)

Харків 2023

ЗАТВЕРДЖЕНО
Науково-методичною радою
Харківського національного
університету внутрішніх справ
Протокол від 30.08.2023 № 7

СХВАЛЕНО
Вченою радою факультету № 6
Протокол від 25.08.2023 № 7

ПОГОДЖЕНО
Секцією Науково-методичної ради
ХНУВС з технічних дисциплін
Протокол від 29.08.2023 № 7

Розглянуто на засіданні кафедри кібербезпеки та DATA-технологій факультету № 6 *(протокол від 15.08.2023 № 8)*

Розробник:
Доцент кафедри, к. т. н., доцент Хавіна І.П.

Рецензенти:
1. Професор кафедри комп'ютерних наук та інформаційних технологій Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут» д. т. н., професор Малєєва О. В.

2. Професор кафедри інформаційних технологій та кібербезпеки ХНУВС, к.т.н., доцент Носов В. В.

1. Розподіл часу навчальної дисципліни за темами (денна форма навчання)

Номер та назва навчальної теми	Кількість годин, відведених на вивчення навчальної дисципліни						Вид контролю
	Всього	з них:					
		Лекції	Семінарські заняття	Практичні заняття	Лабораторні заняття	Самостійна робота	
Семестр № 7							
ТЕМА № 1. *Сутність комплексної системи захисту інформації і принципи її організації*	16	4		2	2	8	
ТЕМА № 2. *Технічне завдання на створення КСЗІ в ІС*	16	4		2	2	8	
ТЕМА № 3. *Оцінка захищеності інформації в ІС від несанкціонованого доступу*	22	4		4	4	10	
ТЕМА № 4. *Особливості проектування КСЗІ для ІТС різних класів*	16	4		2	2	8	
ТЕМА № 5. *Планування захисту інформації в ІС*	18	4		2	4	8	
ТЕМА № 6. *Випробування комплексу технічного захисту інформації та його атестація*	14	2		2	2	8	
ТЕМА № 7. *Управління комплексною системою захисту інформацією в ІС*	20	4		2	4	10	
ТЕМА № 8. *Введення КСЗІ в дію*	14	2		2	2	8	
ТЕМА № 9. *Методи моделювання КСЗІ*	14	2		2	2	8	
Всього за семестр № 7:	150	30		20	24	76	**залік**

2. Методичні вказівки до практичних занять

Практична робота № 1

Тема: Сутність комплексної системи захисту інформації і принципи її організації

Мета роботи: знайомство з основними поняттями із створення комплексної системи захисту інформації в інформаційно-комунікаційній системі. Правові підстави та основні положення щодо створення КСЗІ та комплексу ТЗІ в Україні.

Кількість годин: 2 год.

Місце проведення: комп'ютерний клас.

Навчальні питання:

1. Вступ.
2. Методологічні та концептуальні засади КСЗІ.
3. Етапи створення КСЗІ. Правові підстави для створення КСЗІ.
4. Висновки.

Література:

1. Матеріали лекції 1.

[1, ч. 1, с. 4 – 10]
[1, ч. 2, с. 4 – 18]
[1, ч. 3, с. 4 – 17]

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Зробити огляд завдання і визначити порядок його виконання. Надати посилання на відповідні презентації.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору. У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Завдання на виконання роботи:

Розібратись на основі НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-комунікаційній системі» що таке Комплексна система захисту інформації (КСЗІ); що входить до складу КСЗІ та які служби входять у склад КСЗІ. Ознайомитися зі складом нормативно-правових документів стосовно питання КСЗІ. Запропонувати свою структуру КЗСІ для обраного підприємства.

Теоретичний матеріал

Метою проектування КСЗІ є розробка рекомендацій, організаційних і технічних рішень із забезпечення безпеки інформаційних ресурсів, що зберігаються, обробляються і передаються в каналах зв'язку в комп'ютерних системах та мережах.

Комплексна система захисту інформації (КСЗІ) — сукупність організаційних і інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації в ІТС.

До складу КСЗІ входять заходи та засоби, які реалізують методи, механізми захисту інформації від 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;

Для організації робіт зі створення КСЗІ в ІТС створюється служба захисту інформації, порядок створення, завдання, функції, структура та повноваження якої визначено в НД 1.4-001-2000.

Комплекс засобів захисту (КЗЗ) — сукупність програмно-апаратних засобів, які забезпечують реалізацію політики безпеки інформації.

Закони та норми України вимагають захист інформації, що належить державі, а також інформації з обмеженим доступом, вимоги щодо захисту якої встановлені законом, у тому числі персональні дані.

Комплексна система захисту інформації (КСЗІ) – це організаційні (обов'язкові) та технічні (при необхідності) заходи для захисту інформації від розголошення, витоку та несанкціонованого доступу.

Регулювання створення, впровадження та використання КСЗІ в Україні виконується відповідно до нормативних документів із технічного захисту інформації (далі – НД ТЗІ).

Створення КСЗІ здійснюється згідно з НД ТЗІ 3.7-003-05 "Порядок проведення робіт зі створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі" на підставі технічного завдання, розробленого відповідно до вимог НД ТЗІ 3.7-001-99 "Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі"

Технічне проектування КСЗІ є необхідною умовою для реалізації комплексного підходу щодо забезпечення безпеки. У випадку відсутності

технічного проекту можлива лише реалізація часткових заходів і механізмів безпеки за рахунок яких у сучасних умовах неможливо рішення основних питань інформаційної безпеки.

Технічний проект включає:

1. Пояснювальну записку, яка вміщує опис основних технічних рішень по створенню КСЗІ і організаційних заходів по підготовці КСЗІ до вводу її в дію.

2. Специфікацію на комплекс технічних засобів КСЗІ.

3. Специфікацію на комплекс програмних засобів КСЗІ.

Розробка технічного проекту КСЗІ здійснюється на основі узгодженого з замовником Технічного завдання, а також існуючої Концепції забезпечення ІБ.

Система забезпечення інформаційної безпеки представляє собою сукупність організаційних та програмно-технічних заходів спрямованих на захист інформаційних ресурсів підприємства від різних загроз.

Для досягнення мети проектування необхідно виконати низку кроків. Роботи зі створення і підтримки КСЗІ включають в себе такі етапи:

1. Попереднє дослідження об’єкта інформатизації з метою визначення його поточного стану, розробці вимог по забезпеченню безпеки, документуванню, видачі рекомендацій (Аудит безпеки).

2. Розробка Концепції забезпечення інформаційної безпеки (Політики інформаційної безпеки).

3. Підготовка технічного завдання на створення підсистем КСЗІ (Розробка архітектури КСЗІ та вимог від підсистем).

4. Розробка варіантів технічних рішень.

5. Визначення оптимального проекту КСЗІ (з обґрунтуванням оптимальності).

6. Впровадження проекту.

7. Підтримка та аудит КСЗІ

Для того, щоб виконати аналіз, пропонується такий орієнтовний перелік складових компонентів та підсистем КСЗІ:

1. Зовнішній захищений шлюз і засоби забезпечення міжмережевих взаємодій.

2. Підсистема захисту серверів ЛМ.

3. Засоби захисту робочих станцій.

4. Підсистема моніторингу і аудиту безпеки.

5. Засоби виявлення атак і автоматичного реагування.

6. Підсистема резервного копіювання та відновлення даних.

7. Засоби аналізу захищеності і управління політикою безпеки.

8. Засоби контролю цілісності даних.

9. Засоби криптографічного захисту інформації.

10. Інфраструктура відкритих ключів.

11. Підсистема комплексного антивірусного захисту.

12. Система оновлення ПЗ.

13. Засоби адміністрування безпеки.

14. Засоби технічного захисту інформації.

15. Підсистема організаційного захисту інформації.

16. Нормативна документація, що визначає та регламентує функціонування КСЗІ.

Дані компоненти та підсистеми інтегровані одне в одного, тому допускається й інший поділ на підсистеми КСЗІ, однак при поділі важливо обґрунтувати структуру КСЗІ, що пропонується для аналізу.

Практична робота № 2

Тема № 2. Технічне завдання на створення КСЗІ в АС. Загальні вимоги до розробки технічного завдання на створення КСЗІ в АС.

Мета: знайомство з основними поняттями із створення комплексної системи захисту інформації в інформаційно-комунікаційній системі.

Кількість годин: 2 год.

Місце проведення: комп'ютерний клас.

Література:

1. Матеріали лекції за темою 1.

[2, ч. 1 с. 4 – 11]

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Зробити огляд завдання і визначити порядок його виконання. Надати посилання на відповідні презентації.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору. У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Навчальні питання:

1. Вступ.
2. Вивчення основних принципів побудови технічного завдання.

3. Аналіз зразка технічного завдання на систему захисту інформації об’єкта дослідження.
4. Висновки.

Література:

1. Матеріали лекції 2.

[2, ч. 1, с. 4 – 11]

Матеріально-технічне забезпечення: комп’ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Зробити огляд завдання і визначити порядок його виконання. Надати посилання на відповідні презентації.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору. У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Завдання:

Розробити технічні завдання (ТЗ) за нормативними нормами та вимогами для свого підприємства (НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі та НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в АС).

Практична робота № 3

Тема: Оцінка захищеності інформації в ІС від несанкціонованого доступу. Побудова і структура критеріїв захищеності інформації. Оцінка коректності реалізації послуг безпеки (критерії гарантій).

Мета роботи: Придбання практичних навичок з визначення функціонального профіля та ідентифікації загроз для обраного об’єкта захисту; набуття практичних навичок щодо напрямку реалізації порушником

інформаційних загроз в ІТС. Характеристика типових умов функціонування та вимог із захисту інформації в ІТС.

Кількість годин: 4 год.

Місце проведення: комп'ютерний клас.

Навчальні питання:

1. Вступ.
2. Види критеріїв в НД ТЗІ 2.5-004-99.
3. Рівні кожної послуги.
4. Критерії гарантій середовища розробки.
5. Висновки.

Література:

1. Матеріали лекції 3.

[3, ч. 1 с. 4 – 37]
[3, ч. 2, с. 1 – 11]
[3, ч. 3, с. 1 – 10]

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Зробити огляд завдання і визначити порядок його виконання. Надати посилання на відповідні презентації.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору. У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Завдання на виконання роботи:

Обрати стандартний функціональний профіль для підприємства та пояснити кожну складову профіля.

Практична робота № 4

Тема: Особливості проектування КСЗІ для ІТС різних класів. Класифікація АС.

Мета: знайомство з характеристиками типових умов функціонування та вимог із захисту інформації в ІТС класу 2. Політика реалізації послуг безпеки інформації в ІТС класу 2.

Кількість годин: 2 год.

Місце проведення: комп'ютерний клас.

Навчальні питання:

1. Вступ.
2. Загальні вимоги до процесів обробки в ІТС службової інформації.
3. Типові вимоги до обчислювальної системи ІТС в питаннях захисту інформації.
4. Основні характеристики оброблюваною в ІТС службової інформації.
5. Характеристики технології обробки службової інформації в ІТС.
6. Висновки.

Література:

1. Матеріали лекції 4.

[4, с. 4 – 27]

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Зробити огляд завдання і визначити порядок його виконання. Надати посилання на відповідні презентації.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору. У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Теоретичний матеріал

Модель загроз для інформації, яка планується до циркуляції в АСІ класу 2

В моделі визначені властивості захищеності інформаційних об’єктів, які можуть бути порушеними - конфіденційність (к), цілісність (ц), доступність (д) та якісна оцінка ймовірності здійснення загроз та рівнів збитків (шкоди) по кожному з видів порушень. Потенційні загрози інформації об’єкта інформаційної діяльності наведені в таб. 1.

Таблиця 1.

Модель загроз					
№	Вид загроз	Ймовірність	Що порушує	Рівень шкоди	Механізм реалізації
Моніторинг (розвідка) мережі					
1	Розвідка, аналіз трафіка	Висока	к, ц, д	відсутня	Перехоплення інформації, що пересилаються у незашифрованому виді в широкомовному середовищі передачі даних, відсутність виділеного каналу зв’язку між об’єктами.
Несанкціонований доступ до інформаційних ресурсів із РОМ					
1	Підміна (імітація) довіреного об’єкта або суб’єкта з підробленням мережних адрес тих об’єктів, що атакують	Висока	к, ц, д	середній	Фальсифікація (підроблення мережних адрес IP-адреси, повторне відтворення повідомлень при відсутності віртуального каналу, недостатні ідентифікації та автентифікації при наявності віртуального каналу
2	Зміна маршрутизації	Неприпустимо висока	к, ц, д	низький	Зміна параметрів маршрутизації і змісту інформації, що передається, внаслідок відсутності контролю за маршрутом повідомлень чи відсутності фільтрації пакетів з невірною адресою
3	Селекція потоку інформації й збереження її	висока	к, ц, д	високий	Використанням недоліків алгоритмів віддаленого пошуку шляхом впровадження в розподілену обчислювальну систему хибних об’єктів (атаки типу “людина в середині”).
4	Подолання систем адміністрування доступом до робочих станцій, локальних мереж та захищеного інформаційного об’єкту, заснованих на атрибутах робочих станцій чи засобів	Висока	к, ц, д	високий	Використання недоліків систем ідентифікації та автентифікації, заснованих на атрибутах користувача (ідентифікатори, паролі, біометричні дані та т. ін.). Недостатні ідентифікації та автентифікації об’єктів , зокрема адреси відправника

	управління доступом та маршрутизації (маскування) відповідних мереж (файрволів, проксі - серверів, маршрутизаторів та т.п.).				
Специфічні загрози інформаційним об’єктам					
1	Подолання криптографічної захищеності інформаційних об’єктів, що перехоплені	Низька	К	високий	Використання витоків технічними каналами, вилучення із мережі та специфічних вірусних атак шляхом впровадження програм-шпигунів (spyware) із розкриттям ключових наборів
2	Подолання криптографічної захищеності інформаційних об’єктів робочих станцій	Низька	К	високий	Несанкціонований доступ до інформаційних об’єктів із використанням недоліків систем ідентифікації та автентифікації, заснованих на атрибутах користувача (ідентифікатори, паролі, біометричні дані та т. ін.) із розкриттям ключових наборів
3	Модифікація переданих даних, даних чи програмного коду, що зберігаються в елементах обчислювальних систем.	висока	ц, д	високий	Модифікація чи підміна інформаційних об’єктів (програмних кодів) чи їх частин шляхом впровадження руйнуючих програмних засобів чи зміни логіки роботи програмного файлу із використанням спеціальних типів вірусних атак, спроможних здійснити те чи інше порушення цілісності. Викривлення певної кількості символів інформаційного об’єкту із використанням спеціальних впливів на інформацію технічними каналами в локальній мережі чи в елементах розподіленої мережі
4	Блокування сервісу чи перевантаження запитами системи управління доступом (відмова в обслуговуванні)	висока	Д	високий	Використання атак типу “спрямований шторм” (Syn Flood), передачі на об’єкт, що атакується, не коректних, спеціально підібраних запитів. Використання анонімних (чи із модифікованими адресами) запитів на обслуговування типу електронної пошти (spam) чи вірусних атак спеціального типу

Наявність такої інформації дозволяє побудувати більш предметну загальну модель системи захисту; оцінити значення залишкового ризику, як

функцію захищеності по кожній із функціональних властивостей захищеності; визначити структуру системи захисту та її основні компоненти.

Модель порушника

За порушників на об’єктах інформаційної діяльності розглядаються суб'єкти , внаслідок навмисних або випадкових дій котрих, і (або) випадкові події, внаслідок настання яких можливі реалізації загроз для інформації.

Модель порушника - абстрактний формалізований або неформалізований опис дій порушника, який відображає його практичні та теоретичні можливості, апріорні знання, час та місце дії і та інше. По відношенню до АС порушники можуть бути внутрішніми (з числа співробітників, користувачів системи) або зовнішніми (сторонні особи або будь-які особи, що знаходяться за межами контрольованої зони).

Модель порушника повинна визначати:

- можливу мету порушника та її градацію за ступенями небезпечності для АС;
- категорії осіб, з числа яких може бути порушник.;
- припущення про кваліфікацію порушника;
- припущення про характер його дій.

Метою порушника можуть бути:

- отримання необхідної інформації у потрібному обсязі та асортименті;
- мати можливість вносити зміни в інформаційні потоки у відповідності зі своїми намірами (інтересами, планами);
- нанесення збитків шляхом знищення матеріальних та інформаційних цінностей.

Порушники класифікуються за рівнем можливостей, що надаються їм всіма доступними засобами (табл. 2).

Таблиця 2. Класифікація порушників

№	Можливості порушника по технологічному процесу	Потенційна група порушників	Можливий результат НСД
1	Ні	Службовці, які не мають доступу до інформації, але мають доступ в приміщення (обслуговуючій персонал, відвідувачі)	Перегляд на екрані монітора і розкрадання паперових і машинних носіїв.
2	Запуск задач (програм) з фіксованого набору, що реалізують заздалегідь передбачені функції з обробки інформації.	Більшість користувачів АС, які мають безпосередній доступ до приміщень, з повноваженнями, обмеженими на рівні системи захисту інформації (СЗІ).	Доступ користувача до інформації іншого користувача в його відсутність, в т.ч. через мережу, перегляд інформації на моніторі (недотримання організаційних вимог). Перегляд і розкрадання паперових носіїв.

3	Управління функціонуванням АС, тобто вплив на базове програмне забезпечення ОС і СУБД, на склад і конфігурацію обладнання АС. Робота із зовнішніми носіями.	Адміністратори АС, наділені необмеженими повноваженнями стосовно управління ресурсами.	Доступ адміністратора АС до інформації інших користувачів і до засобів СЗІ, ненавмисне руйнування інформації (недотримання організаційних вимог)
4	Весь обсяг можливостей осіб, які здійснюють ремонт технічних засобів АС.	Обслуговуючий персонал АС. Фахівці сторонніх організацій, які здійснюють постачання і монтаж обладнання для АС.	Доступ обслуговуючого персоналу АС до ПК з інформацією інших користувачів, руйнування інформації, установка закладних пристроїв (недотримання організаційних вимог при ремонті АС).

Визначення конкретних значень характеристик можливих порушників у значній мірі є суб'єктивним. Модель порушника, що побудована з урахуванням особливостей конкретної предметної області і технології обробки інформації, може бути подана перечисленням декількох варіантів його образу. Кожний вид порушника має бути характеризований значеннями характеристик, приведених вище.

Завдання на виконання роботи:

1. До заданих інформаційних ресурсів та інформаційних потоків визначених у попередній роботі визначити перелік загроз (не менше 10).
2. Знайти у загальнодоступних джерелах статистику частоти появи цих загроз.
3. Визначити відповідно до знайденої статистики ймовірність виникнення, кожної загрози.
4. Зробити висновки, щодо адекватності знайденої статистики об’єкту захисту.
5. Визначити зовнішні і внутрішні групи порушників на підприємстві.
6. Обґрунтувати можливі мотиви порушень на підприємстві.

Практична робота № 5
Тема: Планування захисту інформації в ІС.

Мета роботи: Придбання практичних навичок з розробки Плану захисту інформації в ІС. Календарний план робіт з захисту інформації в ІТС.

Кількість годин: 2 год.

Місце проведення: комп’ютерний клас.

Навчальні питання:

1. Вступ
2. Письмове опитування.
3. Призначення та структура Плану захисту інформації в ІС.
4. Календарний план робіт з захисту інформації в ІТС.
5. Висновок.

Література:

1. Матеріали лекції 5.
   [5, с. 4 – 24]

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Зробити огляд завдання і визначити порядок його виконання. Надати посилання на відповідні презентації.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору. У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Завдання на виконання роботи:

Розробити План захисту інформації для підприємства, основуючись на документі Технічне завдання.

Практична робота № 6

Тема: Випробування комплексу технічного захисту інформації та його атестація. Випробування комплексу технічного захисту інформації. Атестація комплексів захисту інформації. Порядок розроблення та оформлення паспорта на комплекс ТЗІ.

Мета роботи: набуття практичних навичок щодо загальних принципів

побудови ТЗ для обраного об’єкта дослідження згідно розробленого технічного завдання на систему захисту інформації (на прикладі).

Кількість годин: 2 год.

Місце проведення: комп’ютерний клас.

Навчальні питання:

1. Вступ
2. Зміст висновків за результатами випробувань комплексу ТЗІ.
3. Склад Програми і методики випробувань комплексу ТЗІ.
4. Атестація комплексу ТЗІ та її види.
5. Етапи атестації комплексу ТЗІ.
6. Акт атестації комплексу ТЗІ.
7. Порядок організації і проведення атестації комплексу ТЗІ.
8. Паспорт на комплекс ТЗІ та його призначення.
9. Висновок.

Література:

1. Матеріали лекції 6.
   [6, с. 4 – 16]

Матеріально-технічне забезпечення: комп’ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Зробити огляд завдання і визначити порядок його виконання. Надати посилання на відповідні презентації.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору. У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Завдання на виконання роботи:

Розробити Програму та методики випробувань для підприємства.

Практична робота № 7

Тема: Управління КСЗІ в ІС.

Мета роботи: набуття практичних навичок щодо призначення, структури і змісту управління КСЗІ. Служба захисту інформації в ІТС: призначення, завдання, функції, повноваження та відповідальність.

Кількість годин: 4 год.

Місце проведення: комп'ютерний клас.

Навчальні питання:

1. Вступ.
2. Мета управління КСЗІ.
3. Особливості систем управління КСЗІ.
4. Завдання та принципи управління КСЗ.
5. Структура управління КСЗІ?
6. Класифікація завдання управління КСЗІ.
7. Висновок.

Література:

1. Матеріали лекції 7.

[7, с. 4 – 31]

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Зробити огляд завдання і визначити порядок його виконання. Надати посилання на відповідні презентації.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору. У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Теоретичний матеріал

Особливості системи управління КСЗІ:

1) призначені для функціонування в конфліктних ситуаціях, оскільки захист інформації є складним двостороннім процесом (КСЗІ _порушник);

2) інформація, на основі якої виробляються управляючі дії (робиться вибір засобів, методів і способів захисту інформації) відрізняється значною неповнотою, недостовірністю і суперечністю;

3) порушники постійно змінюють засоби і методи дії на систему, тактику своїх дій.

Суть управління КСЗІ – цілеспрямована діяльність керівництва організації, посадовців і служби захисту інформації, спрямована на досягнення цілей захисту інформації. Що ж це за цілі?

1. Забезпечення захисту інформації від неправомірного доступу, знищення, модифікування, блокування, копіювання, надання, поширення, а також від інших неправомірних дій відносно такої інформації.

2. Дотримання конфіденційності ІзОД.

3. Реалізація права на доступ до інформації.

4. Забезпечення спостережності та керованості ІТС.

Управління КСЗІ призначене для забезпечення ефективного рішення наступних **задач**:

- запобігання НСД до інформації і передачі її особам, що не мають права на доступ до інформації;
- перекриття витоку інформації, що захищається, технічними каналами і каналів спеціального впливу;
- своєчасне виявлення фактів НСД до інформації;
- попередження можливості несприятливих наслідків порушення порядку доступу до інформації;
- недопущення впливу на технічні засоби обробки інформації, в результаті якого порушується їх функціонування;
- негайне відновлення інформації, модифікованої або знищеної внаслідок НСД до неї;
- постійний контроль за забезпеченням рівня захищеності інформації і гарантій захищеності.

Досягнення основних цілей захисту інформації пов’язане з рішенням круга задач, що становлять **зміст управління КСЗІ**. Основними з них є:

1) безперервне добування, збір, вивчення і аналіз даних обстановки;

2) підтримка системи в постійній готовності до виконання завдань захисту інформації;

3) ухвалення рішень із захисту інформації;

4) доведення завдань до підлеглих;

5) планування заходів захисту інформації;

6) організація і підтримка взаємодії структурних підрозділів організації;

7) усебічне забезпечення заходів захисту інформації;

8) організація управління, під якою розуміється створення системи управління, забезпечення її ефективного функціонування (у тому числі і зашита системи управління від усіх видів дії порушників), а також вдосконалення цієї системи із застосуванням нових інформаційних технологій;

9) управління підготовкою підрозділів захисту інформації;

10) організація і здійснення контролю і допомоги підлеглим.

Дії при управлінні КСЗІ:

Планування

1. Дії щодо ризиків та можливостей – планувати дії, які стосуються ризиків та можливостей, і, як саме, інтегрувати й упровадити ці дії до процесів її СУІБ та оцінювати ефективність цих дій.

а) Оцінка ризиків інформаційної безпеки – визначити та застосовувати процес оцінювання ризиків ІБ, який:

- встановлює та підтримує критерії ризиків ІБ, які містять критерії прийняття ризиків і критерії для виконання оцінки ризиків ІБ;

- гарантує, що повторні оцінки ризиків ІБ призводять до послідовних, дійових та порівняльних результатів;

- ідентифікує ризики ІБ;

- виконує аналіз ризиків інформаційної безпеки;

- оцінює ризики інформаційної безпеки.

б) Оброблення ризиків інформаційної безпеки – визначити та застосовувати процес оброблення ризиків інформаційної безпеки для:

- вибору доречних опцій оброблення ризиків ІБ з урахуванням результатів оцінки ризиків;

- визначити всі заходи безпеки, які необхідно впровадити для вибраної опції оброблення ризиків;

- порівняти ці заходи безпеки з наведеними в стандарті і підтвердити, що не було опущено потрібних заходів безпеки;

- підготувати Положення щодо застосовності, яке містить необхідні заходи безпеки, обґрунтування для їх застосування, впроваджені необхідні заходи безпеки чи ні, обґрунтування для виключень заходів безпеки, наданих у стандарті;

- розробити план оброблення ризиків ІБ;

- отримати від власників ризиків підтвердження плану оброблення ризиків ІБ та згоду на залишкові ризики ІБ.

2. Цілі інформаційної безпеки та планування їх досягнення – встановити цілі ІБ для відповідних функцій та рівнів. Цілі ІБ мають відповідати політиці ІБ; бути вимірюваними (якщо доцільно); враховувати вимоги до ІБ, які

застосовують, а також результати оцінювання ризиків та оброблення ризиків; бути розповсюдженими та оновлюватися.

Під час планування дій для досягнення цілей ІБ визначити: що треба зробити; які ресурси будуть потрібні; хто буде відповідальним; коли процес буде завершено; як результати будуть оцінювати.

Підтримка

1. Ресурси – визначити й забезпечувати наявність ресурсів, потрібних для розроблення, впровадження, підтримання й постійного вдосконалення СУІБ.

2. Компетенція – визначити рівень необхідної компетентності персоналу, який виконує роботи, що впливають на результативність ІБ;

- гарантувати, що цей персонал має компетенцію на основі відповідного навчання, тренінгів або досвіду;

- забезпечувати виконання певних дій для досягнення необхідної компетенції та оцінювати ефективність таких дій;

- зберігати відповідну документовану інформацію як доказ компетентності.

3. Обізнаність. Персонал, який виконує функції під наглядом організації, повинен бути обізнаним в політиці ІБ; його вкладі в ефективність СУІБ, враховуючи переваги від вдосконалення результативності ІБ; розумінні невідповідності вимогам СУІБ.

4. Комунікація – визначити потребу у внутрішніх та зовнішніх комунікаціях з питань СУІБ, включаючи з яких питань спілкуватися; коли спілкуватися; з ким спілкуватися; хто повинен спілкуватися; процеси, за допомогою яких комунікація повинна відбуватися.

5. Документована інформація. СУІБ повинна включати документовану інформацію, визначену стандартом; документовану інформацію, визначену організацією як необхідну для ефективності СУІБ.

Функціонування

1. Робоче планування й контроль: - планувати, впроваджувати й контролювати процеси, необхідні для виконання вимог ІБ, а також впроваджувати заплановані дії;

- впроваджувати плани для досягнення цілей ІБ;

- зберігати документовану інформацію в обсязі, необхідному для впевненості, що процес виконується як було заплановано;

- контролювати заплановані зміни та переглядати наслідки непередбачених змін, застосовуючи дії для усунення будь-яких шкідливих дій, за потреби;

- гарантувати, що процеси, віддані на аутсорсинг, визначені й контрольовані.

2. Оцінювання ризиків інформаційної безпеки – виконувати оцінювання ризиків через заплановані інтервали або коли запропоновані чи відбуваються суттєві зміни з урахуванням визначених критеріїв та зберігати задокументовану інформацію стосовно результатів оцінювання ризиків ІБ.

3. Оброблення ризиків ІБ – впровадити план оброблення ризиків ІБ и зберігати задокументовану інформацію стосовно результатів оброблення ризиків ІБ.

Оцінювання результативності

1. Моніторинг, вимірювання, аналіз та оцінювання – оцінювати результативність ІБ та ефективність СУІБ и визначити:

- що саме потрібно моніторити й вимірювати, включаючи процеси інформаційної безпеки та заходи безпеки;
- методи моніторингу, вимірювань, аналізу та оцінювання, які може бути застосовано для гарантії обґрунтованих результатів;
- коли моніторинг та вимірювання потрібно виконувати;
- хто повинен виконувати моніторинг та вимірювання;
- коли результати моніторингу та вимірювань потрібно аналізувати й оцінювати;
- хто повинен аналізувати й оцінювати ці результати.

2. Внутрішній аудит – проводити внутрішні аудити через заплановані інтервали часу для забезпечення того, що інформація чи СУІБ відповідають власним вимогам організації для її СУІБ та вимогам стандарту; ефективно впроваджена та підтримується;

- планувати, розробляти, впроваджувати та підтримувати програму аудиту, зокрема й частоту, методи, відповідальності, заплановані вимоги та звітність.

Програма аудиту повинна враховувати аналіз важливості процесів, що їх розглядають, і результати попередніх аудитів; визначити критерії аудиту та сферу застосування для кожного аудиту; призначити аудиторів і виконати аудити, які гарантують об'єктивність і неупередженість процесу аудиту; гарантувати, що результати аудиту буде доведено до відповідного керівництва; зберігати документовану інформацію як доказ програми аудиту та результатів аудиту.

3. Перегляд з боку керівництва. Вище керівництво повинно переглядати СУІБ організації через заплановані проміжки часу для гарантування її постійної придатності, адекватності й ефективності. Перегляд з боку керівництва повинен стосуватися розгляду статусу дії, що є наслідком попереднього перегляду керівництва; зміни в зовнішніх та внутрішніх обставинах, які мають відношення до СУІБ; зворотного впливу на результативність ІБ, охоплюючи тенденції в невідповідностях та коригувальних діях, результатах моніторингу та вимірювань, результатах аудиту та досягненнях цілей ІБ; зворотного зв’язку від зацікавлених сторін; результатів оцінювання ризиків і статусу плану оброблення ризиків; можливостей для постійного вдосконалення.

Вихідні дані перегляду з боку керівництва повинні включати рішення стосовно можливостей постійного вдосконалення та будь-яких потреб внесення змін до СУІБ.

Вдосконалення

1. Невідповідності й корегувальні дії – реагувати на невідповідності і за можливості виконувати дії для контролю та їх корекції; вживати заходів щодо наслідків;

- оцінювати потреби в діях для усунення причин невідповідностей для запобігання їх повторення чи виникнення будь-де за допомогою перегляду невідповідностей; визначення причин невідповідностей і визначення, чи існують подібні невідповідності або потенційно можуть з'являтися;
- впровадити певні дії;
- переглянути ефективність виконаних коригувальних дій і внести зміни до СУІБ.

Коригувальні дії мають бути адекватними до наслідків виявлених невідповідностей

2. Постійне вдосконалення– постійно вдосконалювати придатність, адекватність та ефективність СУІБ, гарантування її постійної придатності, адекватності та ефективності.

Завдання на виконання роботи:

Розробити приклад дій стосовно планування (с. 6, пункт 1) для комплексної системи захисту інформації підприємства.

Практична робота № 8

Тема: Введення КСЗІ в дію.

Мета роботи: набуття практичних навичок щодо процесу введення КСЗІ в дію.

Кількість годин: 2 год.

Місце проведення: комп'ютерний клас.

Навчальні питання:

1. Вступ.
2. Письмове опитування студентів.
3. Застосування КСЗІ за призначенням.
4. Технічна експлуатація КСЗІ.
5. Висновки.

Література:

1. Матеріали лекції 8.

[8, с. 4 – 11]

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Зробити огляд завдання і визначити порядок його виконання. Надати посилання на відповідні презентації.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору. У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Теоретичний матеріал

Введення КСЗІ в дію та оцінка захищеності інформації в ІТС

Етап 1. Підготовка КСЗІ до введення в дію

Проводяться роботи з підготовки організаційної структури та розробки розпорядчих документів, що регламентують діяльність із забезпечення захисту інформації в ІТС.

Здійснюється створення СЗІ (призначаються відповідальні особи за захист інформації), якщо цього не було зроблено на попередніх етапах.

Створення СЗІ та розробка Плану захисту здійснюється згідно з НД ТЗІ 1.4-001-2000.

Етап 2. Навчання користувачів

Проводиться навчання користувачів ІТС всіх категорій (технічного обслуговуючого персоналу, звичайних користувачів та користувачів, які мають повноваження щодо управління засобами КСЗІ та ін.) в частині, що їх стосується, основним положенням документів Плану захисту, які необхідні їм для дотримання правил політики безпеки інформації, експлуатації засобів захисту інформації тощо, перевірка їх уміння користуватись впровадженими технологіями захисту інформації і реєстрація результатів навчання.

Етап 3. Пусконалагоджувальні роботи

5.5.2 Монтаж ОТЗ ІТС, кабельного обладнання, мереж живлення та заземлення здійснюється згідно з конструкторською документацією робочого проекту.

5.5.8 Здійснюється згідно з документацією робочого проекту інсталяція, ініціалізація та перевірка працездатності КЗЗ.

Під час інсталяції мають бути задіяні механізми розмежування доступу користувачів до інформації та апаратних ресурсів ІТС, контролю за діями

користувачів, а також контролю цілісності програмного забезпечення.

Етап 4. Попередні випробування

Метою попередніх випробувань є перевірка працездатності КСЗІ та визначення можливості прийняття її у дослідну експлуатацію.

Під час випробувань перевіряються працездатність КСЗІ та відповідність її вимогам ТЗ.

Попередні випробування проводяться згідно з програмою та методиками випробувань. Програму й методики випробувань готує розробник КСЗІ, а узгоджує замовник ІТС. Програма та методики випробувань, протоколи випробувань розробляються та оформлюються згідно з вимогами РД 50-34.698.

Попередні випробування організовує замовник ІТС, а проводить розробник КСЗІ спільно із замовником. Для проведення попередніх випробувань замовником ІТС створюється комісія. Головою комісії призначається представник замовника.

Результати попередніх випробувань оформлюються "Протоколом випробувань", де міститься висновок щодо можливості прийняття КСЗІ у дослідну експлуатацію, а також перелік виявлених недоліків, необхідних заходів з їх усунення, і рекомендовані терміни виконання цих робіт.

Після усунення недоліків у випадку їх наявності та коригування проектної, робочої, експлуатаційної документації КСЗІ оформлюється акт про приймання КСЗІ у дослідну експлуатацію.

Етап 5. Дослідна експлуатація

Під час дослідної експлуатації КСЗІ:

- відпрацьовуються технології оброблення інформації, обігу машинних носіїв інформації,
- керування засобами захисту, розмежування доступу користувачів до ресурсів ІТС та автоматизованого контролю за діями користувачів;
- співробітники СЗІ та користувачі ІТС набувають практичних навичок з використання технічних та програмно-апаратних засобів захисту інформації, засвоюють вимоги організаційних та розпорядчих документів з питань розмежування доступу до технічних засобів та інформаційних ресурсів;
- здійснюється (за необхідністю) доопрацювання програмного забезпечення, додаткове налагоджування та конфігурування КЗЗ;
- здійснюється (за необхідністю) коригування робочої та експлуатаційної документації.

За результатами робіт за довільною формою складається акт про завершення дослідної експлуатації, який містить висновок щодо можливості (неможливості) представлення КСЗІ на державну експертизу.

Етап 6. Державна експертиза КСЗІ

Державна експертиза КСЗІ є окремим етапом приймальних випробувань ІТС. Державна експертиза проводиться з метою визначення відповідності КСЗІ технічному завданню, вимогам НД із захисту інформації та визначення можливості введення КСЗІ в складі ІТС в експлуатацію.

Державна експертиза КСЗІ в ІТС проводиться згідно з Положенням про

державну експертизу в сфері технічного захисту інформації, яке затверджене наказом Адміністрації Держспецзвязку від 16.05.2007 №93 і зареєстроване в Міністерстві юстиції України 16 липня 2007 р. за №820/14087 (нова редакція Положення затверджена наказом Адміністрації Держспецзвязку від 13.10.2017 №565 та перебуває на опрацюванні в Міністерстві юстиції України на предмет можливості державної реєстрації).

Надання послуг щодо проведення Державної експертизи КСЗІ (оцінювання захищеності інформації) підлягає ліцензуванню відповідно до Переліку послуг у галузі технічного захисту інформації, господарська діяльність щодо надання яких підлягає ліцензуванню.

Виявлені під час державної експертизи недоліки усуваються до її завершення, порядок усунення такий самий, як і для попередніх випробувань. Якщо в силу якихось причин усунути недоліки в ході експертизи неможливо, це оформлюється актом, до якого вноситься перелік необхідних доробок та рекомендації щодо їх виконання. Після завершення передбачених актом робіт проводиться повторна експертиза.

Для інтегрованих ІТС може проводитись державна експертиза кожної складової частини (модуля) КСЗІ окремо.

Якщо інтегрована КСЗІ має у своєму складі типові модулі, які створювались за єдиним ТЗ, то експертиза таких модулів КСЗІ виконується в два етапи: на першому проводиться у повному обсязі експертиза одного обраного типового модуля, а на другому – здійснюється перевірка відповідності умов експлуатації типовим на кожному конкретному об’єкті для всіх модулів КСЗІ цього типу.

Введення до складу діючої КСЗІ нового (оціненого) модуля здійснюється без проведення повторної експертизи всієї КСЗІ.

Проводиться оцінювання взаємодії нового модуля зі складовими частинами КСЗІ, які вже знаходяться в експлуатації.

Допускається розпочинати і проводити державну експертизу КСЗІ паралельно з роботами етапів проектування.

Завдання на виконання роботи:

Описати процес введення КСЗІ в дію та оцінити рівень захищеності інформації на підприємстві.

Практична робота № 9

Тема: Методи моделювання КСЗІ.

Мета роботи: набуття практичних навичок щодо моделювання КСЗІ. Вибір показників ефективності та критеріїв оптимальності КСЗІ та оцінити рівень захищеності інформації в АС.

Кількість годин: 2 год.

Місце проведення: комп’ютерний клас.

Навчальні питання:

1. Вступ.
2. Письмове опитування студентів.
3. Типи моделювання КСЗІ. Особливості моделювання КСЗІ.
4. Основні етапи оцінювання КСЗІ.
5. Показники ефективності системи та вимоги до них.
6. Приклади критеріїв придатності, оптимальності й раціональності.
7. Підходи, що використовують для оцінки ефективності КСЗІ.
8. Висновки.

Література:

1. Матеріали лекції 9.

[9, с. 4 – 18]

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Зробити огляд завдання і визначити порядок його виконання. Надати посилання на відповідні презентації.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору. У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Завдання на виконання роботи:

Запропонуйте оцінку ефективності для своєї КСЗІ. Визначить показники ефективності КСЗІ.

3. Рекомендована література (основна, додаткова), інформаційні та навчальні ресурси в Інтернеті

Основна література

1. Козюра В.Д. Комплексні системи захисту інформації в інформаційно-телекомунікаційних системах: навчальний посібник / В.Д. Козюра, В.О. Хорошко, М. Є. Шелест, Ю. М. Ткач, Я.Ю. Усов. – Ніжин: ФОП Лук'яненко В.В., ТПК «Орхідея», 2019. – 144 с.
2. Остапов С. Е. Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2018. – 476 с.
3. Комплексні системи захисту інформації : навчальний посібник /[Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В.] – Вінниця : ВНТУ, 2018. – 118 с.

Додаткова література

1. ДСТУ 33960-96 Захист інформації. Технічний захист інформації. Основні положення.
2. ДСТУ 33961-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт.
3. ДСТУ 33962-97 Захист інформації. Технічний захист інформації. Терміни та визначення;
4. НД ТЗІ 1.1-005-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.
5. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі.
6. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.
7. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.
8. НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.
9. НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в АС.
10. НД ТЗІ 1.6-004-2013 Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що становить державну таємницю.

Інформаційні ресурси в Інтернеті:

1. Державна служба спеціального зв'язку та захисту інформації (ДСЗЗІ) [Електронний ресурс]. – Режим доступу: https://cip.gov.ua/ua
2. Ю.Є. Яремчук, П.В. Павловський, В.С. Катаєв, В.В. Сінюгін. Комплексні системи захисту інформації / Навчальний посібник.

[Електронний ресурс]. – Режим доступу: https://web.posibnyky.vntu.edu.ua/fmib/41yaremchuk_kompleksni_systemy_zahystu_informaciyi/