МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

Кафедра кібербезпеки та DATA-технологій, факультет №6

МЕТОДИЧНІ МАТЕРІАЛИ

ДО ЛАБОРАТОРНИХ ЗАНЯТЬ

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 лабораторних занять

Лабораторна робота № 1

Тема: Дослідження структури об'єкту захисту

Мета роботи: Придбання теоретичних знань та практичних навичок з аналізу структури об'єкта захисту (обстеження об'єкта).

Кількість годин: 2 год.

Місце проведення: комп'ютерний клас.

Навчальні питання:

Вступ.

1. Обстеження індивідуального об'єкту АС.
2. Етапи створення КСЗІ. Правові підстави для створення КСЗІ.

Висновки.

Література:

1. Матеріали лекції 1.

[1, ч. 1 с. 8 – 12, 16 - 19]

[1, ч. 2, с. 5 - 9]

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.

Теоретичні відомості

Першим кроком при створені КСЗІ є визначення того, що саме буде захищатись, тобто дослідження об'єкта, для якого проектуватиметься система захисту. Тому розв'язок задачі аналізу об'єкту захисту є обов'язковою складовою процесу проектування КСЗІ. Даний етап проектування дозволяє визначити та ідентифікувати інформаційні ресурси та інформаційні потоки, що присутні на об'єкті захисту, а також небезпечні фактори, вразливості та небезпеки, що впливають та загальний стан безпеки об'єкту через конкретні інформаційні ресурси чи інформаційні потоки, які згодом будуть використані

для моделювання об’єкта захисту та прийняття відповідних технічних рішень з ПКСЗІ. Саме тому, якість результату процесу ПКСЗІ істотно залежить від правильності окреслення об’єкта захисту та якості аналізу його структури. В зв’язку з тим, що проектування систем значною мірою є мистецтвом, тому не існує уніфікованої методики аналізу об’єкта. Водночас існує низка рекомендацій з цього приводу, зокрема в Україні діє стандарт ДСТУ 3396.1-96, що регулює порядок проведення дослідження технічного захисту інформації на об’єктах (розділ 4).

Аналіз об’єкта повинен бути комплексним, оскільки стійкість системи визначається найслабшою ланкою. Тому, крім аналізу технічної підсистеми об’єкту необхідно виконати аналіз персоналу, програмного забезпечення, комп’ютерної мережі тощо. Аналіз персоналу включає визначення характеру інформації, що циркулює в межах структурних підрозділів, підпорядкування на об’єкті, доступ персоналу до інформаційних ресурсів. Аналіз програмного забезпечення передбачає аналіз захищеності робочих станцій, розмежування прав доступу до них, антивірусний захист, наявність дірок, чорних ходів тощо. Аналіз комп’ютерної мережі має на меті визначення місць витоку інформації, циркулювання інформації мережею, наявних засобів захисту від зовнішніх та внутрішніх атак.

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.

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:

1. Виконати дослідження об’єкта з метою визначення його складових, структурних підрозділів.

2. Представити структурну схему досліджуваного об’єкту, з ідентифікацією та аналізом інформаційних потоків та інформаційних ресурсів.

3. Визначити тип технологій передачі інформації на об’єкті (автоматизована, автоматична, за допомогою персоналу тощо) для кожного інформаційного потоку.

4. Визначити носії інформації, що використовуються для зберігання інформаційних ресурсів, та методи й засоби їх захисту.

5. Зробити загальні висновки, щодо необхідності захисту інформаційних ресурсів підприємства.

6. Результат виконання роботи представити у вигляді звіту.

Індивідуальні завдання

1. Розробка комплексної системи захисту інформації для агентства з продажу нерухомості.

2. Розробка комплексної системи захисту інформації для кредитного відділу комерційного банку.

3. Розробка комплексної системи захисту інформації для бухгалтерії вищого навчального закладу.

4. Розробка комплексної системи захисту інформації для ГО.

5. Розробка комплексної системи захисту інформації для інтернет-магазину продажу електротоварів.

6. Розробка комплексної системи захисту інформації для відділу кадрів комерційного банку.

7. Розробка комплексної системи захисту інформації для відділення фірми інтернет-провайдера.

8. Розробка комплексної системи захисту інформації для відділення комерційного банку.

9. Розробка комплексної системи захисту інформації для приватної конструкторської фірми.

10. Розробка комплексної системи захисту інформації для сховища даних супермаркету.

11. Розробка комплексної системи захисту інформації для клінічної лабораторії.

12. Розробка комплексної системи захисту інформації для бібліотечного репозиторію кафедри.

13. Розробка комплексної системи захисту інформації для будівельної організації.

14. Розробка комплексної системи захисту інформації для аптеки.

15. Розробка комплексної системи захисту інформації для ректорату вищого навчального закладу.

16. Розробка комплексної системи захисту інформації для кафедри вищого навчального закладу.

17. Розробка комплексної системи захисту інформації для факультету вищого навчального закладу.

18. Розробка комплексної системи захисту інформації для ветеринарної клініки.

19. Розробка комплексної системи захисту інформації для страхової компанії.

20. Розробка комплексної системи захисту інформації для інтернет-магазину оптової продажу одягу.

21. Розробка комплексної системи захисту інформації для відділу кадрів навчального закладу.

22. Розробка комплексної системи захисту інформації для фірми інтернет-провайдера.

23. Розробка комплексної системи захисту інформації для відділення магазину мережи «Сільпо».

24. Розробка комплексної системи захисту інформації для приватної конструкторської фірми.

25. Розробка комплексної системи захисту інформації для бібліотечного порталу вищого навчального закладу.

26. Розробка комплексної системи захисту інформації для транспортної компанії (вантажні перевозки).

27. Розробка комплексної системи захисту інформації для служби таксі.

28. Розробка комплексної системи захисту інформації для відділення пошти.

29. Розробка комплексної системи захисту інформації для станції пасажирських автобусних перевезень.

30. Розробка комплексної системи захисту інформації для спортивного комплексу.

Лабораторна робота № 2

Тема: Модель порушника.

Мета роботи: Придбання опанування практичних навичок з визначення та ідентифікації загроз для заданого об’єкта захисту.

Кількість годин: 2 год.

Місце проведення: комп’ютерний клас.

Навчальні питання:

Вступ.

1. Ідентифікації загроз для заданого об’єкта захисту.
2. Модель порушника.

Висновок.

Література:

1. Матеріали лекцій

[2, 2 ч. с. 15]

[3, 1 ч., с. 3 - 15]

Матеріально-технічне забезпечення занять: комп’ютерна мережа із підключенням до Intertnet.

Заняття проводиться в комп’ютерному класі. Кожний студент забезпечується окремим робочим місцем (комп’ютером, підключеним до локальної мережі та із підключенням до Internet). Методичне забезпечення, індивідуальні завдання надаються в електронному вигляді через локальну комп’ютерну мережу університету.

Підготовка до заняття

Вивчити загальні питання організації та функціонування систем технічного захисту інформації.

II. 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.

Теоретичні відомості

Порушник – це особа, яка може отримати доступ до роботи з включеними в склад АС засобами. Вона може помилково, унаслідок необізнаності, цілеспрямовано, за злим умислом або без нього, використовуючи різні можливості, методи та засоби здійснити спробу

виконати операції, які призвели або можуть призвести до порушення властивостей інформації, що визначені політикою безпеки.

Зрозуміло, що в кожному конкретному випадку для кожного об’єкта визначаються імовірні загрози і моделі потенціальних порушників – «провідників» цих загроз, включаючи можливі сценарії їх здійснення. Цей етап дуже складний, оскільки від служби безпеки необхідно для кожного об’єкта вибрати з декількох можливих типів порушників один, на який і буде орієнтована система безпеки, що проектується. Відповідно до нормативних документів модель порушника – це абстрактний формалізований або неформалізований опис порушника.

Модель порушника відображає його практичні та потенційні можливості, апріорні знання, час та місце дії тощо.

При розробці моделі порушника визначаються:

- припущення щодо категорії осіб, до яких може належати порушник;
- припущення щодо мотивів дій порушника (цілей, які він переслідує);
- припущення щодо рівня кваліфікації та обізнаності порушника та його технічної оснащеності (щодо методів та засобів, які використовуються при здійсненні порушень);
- обмеження та припущення щодо характеру можливих дій порушників (за часом та місцем дії та інші).

Припускається, що у своєму рівні порушник – це фахівець вищої кваліфікації, який має повну інформацію про систему.

Звичайно розглядаються 5 типів порушників. Спочатку їх поділяють на дві групи: зовнішні і внутрішні порушники. Зовнішні порушники включають:

- добре озброєну й оснащену силову групу, що діє зовні швидко і напролом;
- поодинокий порушник, що не має допуску на об'єкт і намагається діяти потайки й обережно, так як він усвідомлює, що сили реагування мають перед ним переваги.

Серед потенціальних внутрішніх порушників можна відзначити:

 допоміжний персонал об'єкту, що допущений на об'єкт, але не допущений до життєвоважливого центру АС;

 основний персонал, що допущений до життєво важливого центру (найбільш небезпечний тип порушників);

 співробітників служби безпеки, які часто формально і не допущені до життєво важливого центру, але реально мають достатньо широкі можливості для збору необхідної інформації і скоєння акції.

Серед внутрішніх порушників можна виділити наступні категорії персоналу:

- користувачі (оператори) системи;
- персонал, що обслуговує технічні засоби (інженери, техніки);
- співробітники відділів розробки та супроводження ПЗ (прикладні та системні програмісти);

- технічний персонал, що обслуговує будівлю (прибиральниці, електрики, сантехніки та інші співробітники, що мають доступ до будівлі та приміщення, де розташовані компоненти АС);
- співробітники служби безпеки;
- керівники різних рівнів та посадової ієрархії.

- Сторонні особи, що можуть бути порушниками:
- клієнти (представники організацій, громадяни);
- відвідувачі (запрошені з якого-небудь приводу);
- представники організацій, взаємодіючих з питань забезпечення життєдіяльності організації (енерго-, водо-, теплопостачання і т.д.);
- представники конкуруючих організацій (іноземних служб) або особи, що діють за їх завданням;
- особи, які випадково або навмисно порушили пропускний режим (без мети порушити безпеку);
- будь-які особи за межами контрольованої зони.

Можна виділити також три основних мотиви порушень: безвідповідальність, самоствердження та з корисною метою.

При порушеннях, викликаних *безвідповідальністю*, користувач цілеспрямовано або випадково виробляє руйнуючі дії, які не пов'язані проте зі злим умислом. У більшості випадків це наслідок некомпетентності або недбалості. Деякі користувачі вважають одержання доступу до системних наборів даних значним успіхом, затіваючи свого роду гру «користувач - проти системи» заради *самоствердження* або у власних очах, або в очах колег.

Порушення безпеки АС може бути викликано *корисливим інтересом* користувача системи. У цьому випадку він буде цілеспрямовано намагатися перебороти систему захисту для доступу до інформації в АС. Навіть якщо АС має засоби, що роблять таке проникнення надзвичайно складним, цілком захистити її від проникнення практично неможливо.

Таблиця 1.

Класифікація	Характеристики
За рівнем знань про АС	- знає функціональні особливості АС, основні закономірності формування в ній масивів даних і потоків запитів до них, уміє користуватися штатними засобами; - має високий рівень знань і досвід роботи з технічними засобами системи і їх обслуговуванням; - має високий рівень знань в області програмування й обчислювальної техніки, проектування й експлуатації автоматизованих інформаційних систем; - знає структуру, функції і механізм дії засобів захисту, їх сильні і слабкі сторони.
За рівнем можливостей (методам і засобам	- застосовує чисто агентурні методи отримання відомостей; - застосовує пасивні засоби (технічні засоби перехоплення без модифікації компонентів системи);

що використовуються).	- використовує тільки штатні засоби та недоліки системи захисту для її подолання (несанкціоновані дії з використанням дозволених засобів), а також компактні магнітні носії інформації, які можуть бути тайком пронесені крізь пости охорони; - застосовує методи та засоби активного впливу (модифікація та підключення додаткових технічних засобів, підключення до каналів передавання даних, впровадження програмних закладок та використання спеціальних інструментальних та технологічних програм).
За часом дії	- у процесі функціонування (під час роботи компонент системи); - у період неактивності системи (у неробочий час, під час планових перерв у її роботі, перерв для обслуговування та ремонтів і т.д.); - як у процесі функціонування, так і в період неактивності компонент системи.
За місцем дії	- без доступу на контрольовану територію організації; - з контрольованої території без доступу до будівель та споруджень; - усередині приміщень, але без доступу до технічних засобів; - з робочих місць кінцевих користувачів (операторів); - з доступом у зону даних (баз даних, архівів і т.д.); - з доступом у зону управління засобами забезпечення безпеки.

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.

III. 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:

1. Визначити зовнішні і внутрішні групи порушників на підприємстві.
2. Обґрунтувати можливі мотиви порушень на підприємстві.
3. Розробити модель порушника.

Відповідно до таблиці 1 та до індивідуального завдання заповнити таблицю 2.

Таблиця 2.

Визначення категорії	Мотив порушення	Рівень кваліфікації та обізнаності щодо АС.	Можливості використання засобів та методів подолання системи захисту.	Специфікація моделі порушника за часом дії	Специфікація моделі порушника за місцем дії	Сумарний рівень загрози
Внутрішні по відношенню до АС						
…..						

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.

Лабораторна робота № 3

Тема : Моделі загроз. Класифікації моделі загроз.

Мета : Розглянути питання оцінки дій загроз в інформаційних системах

Кількість годин: 4 год.

Місце проведення: комп’ютерний клас.

Навчальні питання:

1. Види загроз.
2. Визначення впливу кожного фактору на стан ІБ.
3. Процедури ранжування.
4. Ймовірностей появи головної події.
5. Метод оцінки ризиків на основі моделі загроз і вразливостей

Література:

1. Матеріали лекції 3

[3, 1 ч. с. 6 – 17]
[3, 2 ч., с. 2 - 11]
[3, 3 ч., с. 3 - 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.

Стислі теоретичні відомості

Після ідентифікації негативних факторів, що впливають на критичні інформаційні потоки та ресурси об’єкта захисту, а відтак і на його загальний стан інформаційної безпеки, необхідно визначити інтегральний показник їх впливу. Для досягнення цієї мети використовується методи математичного моделювання, з якими можна детально ознайомитись у літературі, рекомендованій для виконання даної роботи, або у іншій з даної тематики.

Результатом оцінювання стану інформаційної безпеки є не лише визначення загального стану, але й визначення впливу кожного фактору на цей стан. Останнє визначається за допомогою процедури ранжування. Для розрахунків рангів передбачається використання різниць ймовірностей появи головної події та її ймовірності у випадку вилучення події, ранг якої розраховується:

$$Rngi = P - Pi,$$

де P – ймовірність появи головної події; Pi – ймовірність появи головної події за умови вилучення i-тої події (ймовірність її виникнення дорівнює нулю).

На основі отриманого масиву значень різниць $Rngi$ визначають найбільше значення з масиву та задають ранг для подій, яким відповідає дане значення різниці найвище значення рангу – один, після чого дані події вилучають з масиву. За аналогічним алгоритмом визначають події з наступним значенням рангу.

Дана процедура повторюється доти, доки потужність масиву не буде рівною нулю. В результаті даних розрахунків можна буде зробити висновок про значущість загроз для загальної інформаційної захищеності об’єкту.

Хід роботи
Метод оцінки ризиків на основі моделі загроз і вразливостей

Для того, щоб оцінити ризик інформації, **аналізуються всі загрози**, які діють на інформаційну систему, і уразливості, через які можлива реалізація загроз.

Виходячи з введених власником інформаційної системи даних, **будується модель загроз і вразливостей**, актуальних для інформаційної системи компанії.

На основі отриманої моделі проводиться **аналіз ймовірності реалізації загроз інформаційної безпеки на кожен ресурс** і, виходячи з цього, розраховуються ризики.

Основні поняття та припущення моделі

Базові загрози інформаційній безпеці - порушення конфіденційності, порушення цілісності та відмова в обслуговуванні.

Ресурс - будь-який контейнер, призначений для зберігання інформації, схильний до погроз інформаційної безпеки (сервер, робоча станція, переносний комп'ютер).

Властивостями ресурсу є: перелік загроз, які впливають на нього, і критичність ресурсу.

Загроза - дія, яка потенційно може привести до порушення безпеки.

Властивістю загрози є перелік вразливостей, за допомогою яких може бути реалізована загроза.

Уразливість - це слабке місце в інформаційній системі, що може привести до порушення безпеки шляхом реалізації певної загрози. Властивостями уразливості є: ймовірність (простота) реалізації загрози через дану уразливість і критичність реалізації загрози через дану уразливість.

Критичність ресурсу (D) - збиток, який понесе компанія від втрати ресурсу. Здається в рівнях (кількість рівнів може бути в діапазоні від 2 до 100) або в грошах. Залежно від обраного режиму роботи, може складатися з **критичності ресурсу по конфіденційності, цілісності та доступності (Dc, Di, Da)**.

Критичність реалізації загрози (ER) - ступінь впливу реалізації загрози на ресурс, тобто як сильно реалізація загрози вплине на роботу ресурсу. Здається в процентах. Складається з **критичності реалізації загрози по конфіденційності, цілісності та доступності (ERc, ERi, ERa**).

Імовірність реалізації загрози через дану уразливість в протягом року (P (V)) - ступінь можливості реалізації загрози через дану уразливість в тих чи інших умовах. Вказується у відсотках.

Максимальна критичний час простою (Tmax) - значення часу простою, яке є критичним для організації. Тобто збиток, нанесений організації при простоюванні ресурсу протягом критичного часу простою, максимальний. При простоюванні ресурсу протягом часу, що перевищує критичне, збиток, нанесений організації, не збільшується.

Розрахунок ризиків за загрозою інформаційної безпеки

На першому етапі розраховується рівень загрози по уразливості *Th* на основі критичності і ймовірності реалізації загрози через дану уразливість.

Рівень загрози показує, наскільки критичним є вплив даної загрози на ресурс з урахуванням ймовірності її реалізації.

Для того, щоб оцінити ризик інформації, **аналізуються всі загрози**, які діють на інформаційну систему, і уразливості, через які можлива реалізація загроз.Виходячи з введених власником інформаційної системи даних, **будується модель загроз і вразливостей**, актуальних для інформаційної системи компанії.

На основі отриманої моделі проводиться **аналіз ймовірності реалізації загроз інформаційної безпеки на кожен ресурс** і, виходячи з цього, розраховуються ризики.

Основні поняття та припущення моделі

Базові загрози інформаційній безпеці - порушення конфіденційності, порушення цілісності та відмова в обслуговуванні.

Ресурс - будь-який контейнер, призначений для зберігання інформації, схильний до погроз інформаційної безпеки (сервер, робоча станція, переносний комп'ютер).

Властивостями ресурсу є: перелік загроз, які впливають на нього, і критичність ресурсу.

Загроза - дія, яка потенційно може привести до порушення безпеки.

Властивістю загрози є перелік вразливостей, за допомогою яких може бути реалізована загроза.

Уразливість - це слабке місце в інформаційній системі, що може привести до порушення безпеки шляхом реалізації певної загрози. Властивостями уразливості є: ймовірність (простота) реалізації загрози через дану уразливість і критичність реалізації загрози через дану уразливість.

Критичність ресурсу (D) - збиток, який понесе компанія від втрати ресурсу. Здається в рівнях (кількість рівнів може бути в діапазоні від 2 до 100) або в грошах. Залежно від обраного режиму роботи, може складатися з **критичності ресурсу по конфіденційності, цілісності та доступності (Dc, Di, Da)**.

Критичність реалізації загрози (ER) - ступінь впливу реалізації загрози на ресурс, тобто як сильно реалізація загрози вплине на роботу ресурсу. Здається в процентах. Складається з **критичності реалізації загрози по конфіденційності, цілісності та доступності (ERc, ERi, ERa**).

Імовірність реалізації загрози через дану уразливість в протягом року (P (V)) - ступінь можливості реалізації загрози через дану уразливість в тих чи інших умовах. Вказується у відсотках.

Максимальна критичний час простою (Tmax) - значення часу простою, яке є критичним для організації. Тобто збиток, нанесений організації при простоюванні ресурсу протягом критичного часу простою, максимальний.

При простоюванні ресурсу протягом часу, що перевищує критичне, збиток, нанесений організації, не збільшується.

Розрахунок ризиків за загрозою інформаційної безпеки

1. На першому етапі розраховується рівень загрози по уразливості *Th* на основі критичності і ймовірності реалізації загрози через дану уразливість.

Рівень загрози показує, наскільки критичним є вплив даної загрози на ресурс з урахуванням ймовірності її реалізації.

$$Th_{c,i,a} = \frac{ER_{c,i,a}}{100} x \frac{P(V)_{c,i,a}}{100},$$

де $ER_{c,i,a}$ - критичність реалізації загрози (%);

$P(V)_{c,i,a}$ – ймовірність реалізації загрози через дану вразливість.

Обчислюється одне або три значення залежно від кількості базових загроз. Виходить значення рівня ***загрози по уразливості*** в інтервалі від 0 до 1.

Для розрахунку рівня загрози за всіма вразливостями *CTh*, через які можлива реалізація даної загрози на ресурсі, підсумовуються отримані рівні загроз через конкретні уразливості за такою формулою:

$$CTh = 1 - \prod_{i=1}^{n}(1 - Th),$$

Для режиму з трьома базовими загрозами:

$$CThc = 1 - \prod_{i=1}^{n}(1 - Thc),$$
$$CThi = 1 - \prod_{i=1}^{n}(1 - Thi),$$
$$CTha = 1 - \prod_{i=1}^{n}(1 - Tha),$$

Значення рівня загрози за всіма вразливістю виходять в інтервалі від 0 до 1.

3. Аналогічно розраховується загальний рівень загроз ресурсу CTh_{R} (враховуючи всі загрози, що діють на ресурс):

Для режиму з однією базовою загрозою:

$$CThR = 1 - \prod_{i=1}^{n}(1 - Th),$$

Для режиму з трьома базовими загрозами:

$$CThRc = 1 - \prod_{i=1}^{n}(1 - Thc),$$
$$CThRi = 1 - \prod_{i=1}^{n}(1 - Thi),$$
$$CThRa = 1 - \prod_{i=1}^{n}(1 - Tha),$$

Значення загального рівня загрози виходить в інтервалі від 0 до 1.

4. Ризик за ресурсом R розраховується так.

Для режиму з однією базовою загрозою:

$$R = \mathrm{C}ThR\ x\ D,$$

де D – критичність ресурсу. Задається в грошах чи рівнях.
У разі загрози доступність (відмова в обслуговуванні) критичність ресурсу на рік обчислюється за такою формулою:

$$D_{a/\text{рік}} = D_{a/\text{год}}\ x\ T,$$

Для інших загроз критичність ресурсу задається на рік.
Для режиму з трьома базовими загрозами:

$$Rc = \mathrm{C}ThRc\ x\ Dc,$$
$$Ri = \mathrm{C}ThRi\ x\ Di,$$
$$Ra = \mathrm{C}ThRa\ x\ Da,$$

де $D_{c,i,a}$ – критичність ресурсу за трьома загрозами. Задається в грошах чи рівнях.

Сумарний ризик за трьома загрозами:

$$R = (1 - \prod_{i=1}^{3}(1 - \frac{Ri}{100}))x100.$$

Таким чином, виходить значення ризику ресурсу в рівнях (заданих користувачем) або грошах.

5. Ризик по інформаційній системі CR

Для режиму з однією базовою загрозою:
- для режиму роботи в грошах:

$$\mathrm{C}R = \sum_{i=1}^{n} R_i,$$

- для режиму роботи у рівнях:

$$CR = (1 - \prod_{i=1}^{n}(1 - \frac{Ri}{100}))x100.$$

Для режиму роботи з трьома загрозами:
- для режиму роботи в грошах:

$$\mathrm{C}R_{a,c,i} = \sum_{i=1}^{n} R_i,$$
$$CR = \sum_{i=1}^{n} \mathrm{C}R_{a,c,i},$$

$\mathrm{C}R_{a,c,i}$ - ризик по системі по кожному виду загроз;
CR - ризик по системі по кожному виду загроз.
- для режиму роботи на рівнях:

$$CR_{a,i,c} = (1 - \prod_{i=1}^{n}(1 - \frac{Ri}{100}))x100.$$

$$CR = (1 - \prod_{i=1}^{3}(1 - \frac{R_{a,i,c}}{100}))x100.$$

Завдання контрзаходів

Для розрахунку ефективності введеного контрзаходу необхідно пройти послідовно по всьому алгоритму з урахуванням заданого контрзаходу. Тобто, на виході користувач отримує значення двох ризиків – ризику без урахування контрзаходу *Rold* та ризик з урахуванням заданого контрзаходу *Rnew* (або з урахуванням того, що вразливість закрита).

Ефективність введення контрзаходу *E* розраховується за формулою:

$$E = \frac{R_{old} - R_{new}}{R_{old}}$$

В результаті роботи алгоритму користувач системи отримує такі дані:

• Ризик за трьома базовими загрозами (або однією сумарною загрозою) для ресурсу;

• Ризик сумарно за всіма загрозами ресурсу;

• Ризик за трьома базовими загрозами (або однією сумарною загрозою) для інформаційної системи;

• Ризик усіх загроз для інформаційної системи;

• Ризик усіх загроз для інформаційної системи після завдання контрзаходів;

• Ефективність контрзаходу;

• Ефективність комплексу контрзаходів.

Приклад розрахунку ризику інформаційної безпеки на основі моделі загроз та вразливостей

Ресурс	Загрози	Вразливість
Сервер (критичность ресурса 100 у.е.)	**Загроза 1** Неавторизоване проникнення порушника всередину периметра, що охороняється (одного з периметрів)	**Вразливість 1** Відсутність регламенту доступу до приміщень з ресурсами, що містять цінну інформацію
		Вразливість 2 Відсутність системи спостереження (відеоспостереження, сенсори тощо) за об'єктом (або існуюча система спостереження охоплює не всі важливі об'єкти)
	Загроза 2 Неавторизована модифікація інформації в системі електронної пошти, що зберігається на ресурсі	**Вразливість 1** Відсутність авторизації для внесення змін до системи електронної пошти
		Вразливість 2 Відсутність регламенту роботи із системою криптографічного захисту електронної кореспонденції
	Загроза 3 Розголошення конфіденційної інформації співробітниками компанії	**Вразливість 1** Відсутність угод про конфіденційність
		Вразливість 2 Розподіл атрибутів безпеки (ключ доступу, шифрування) між кількома довіреними співробітниками

Вхідні данні

Ресурси АС	**Загроза/Вразливість**	**Ймовірність реалізації через дану вразливість за рік (%), *P(V)***	**Критичність реалізації загрози через вразливість (%), *ER***
1	Загроза1/Вразливість1	50	60
	Загроза1/Вразливіст2	20	60
	Загроза2/Вразливість1	60	40
	Загроза2/Вразливіст2	10	40
	Загроза3/Вразливість1	10	80
	Загроза3/Вразливіст2	80	80
2	Загроза1/Вразливість1	10	60
	Загроза1/Вразливіст2	20	60
	Загроза2/Вразливість1	20	40
	Загроза2/Вразливіст2	60	40
	Загроза3/Вразливість1	10	80
	Загроза3/Вразливіст2	80	80

Рівень по загрозам

Ресурси АС	**Загроза/Вразливість**	**Рівень загрози (%), *Th***	**Рівень загрози за всіма вразливастями, що реалізують дану загрозу (%), *CTh***
1	Загроза1/Вразливість1	0,30	0,38
	Загроза1/Вразливіст2	0,12	
	Загроза2/Вразливість1	0,24	0,27
	Загроза2/Вразливіст2	0,04	
	Загроза3/Вразливість1	0,08	0,67
	Загроза3/Вразливіст2	0,64	
2	Загроза1/Вразливість1	0,06	0,17
	Загроза1/Вразливіст2	0,12	
	Загроза2/Вразливість1	0,08	0,30
	Загроза2/Вразливіст2	0,24	
	Загроза3/Вразливість1	0,08	0,67
	Загроза3/Вразливіст2	0,64	

Рівень по ресурсам

Ресурси АС	**Загроза/Вразливість**	**Рівень загрози за всіма вразливастями, що реалізують дану загрозу (%), *CTh***	**Загальний рівень загроз по ресурсу (%), *CThR***
1	Загроза1/Вразливість1	0,38	0,85
	Загроза1/Вразливіст2		
	Загроза2/Вразливість1	0,27	
	Загроза2/Вразливіст2		
	Загроза3/Вразливість1	0,67	
	Загроза3/Вразливіст2		
2	Загроза1/Вразливість1	0,17	0,81
	Загроза1/Вразливіст2		
	Загроза2/Вразливість1	0,30	
	Загроза2/Вразливіст2		
	Загроза3/Вразливість1	0,67	
	Загроза3/Вразливіст2		

Ризик по ресурсам

Ресурси АС	**Загроза/Вразливість**	**Загальний рівень загроз по ресурсу (%), *CThR***	**Ризик ресурсу (у.о), *R***
1	Загроза1/Вразливість1	0,851	85,11
	Загроза1/Вразливіст2		
	Загроза2/Вразливість1		
	Загроза2/Вразливіст2		
	Загроза3/Вразливість1		
	Загроза3/Вразливіст2		
2	Загроза1/Вразливість1	0,808	80,84
	Загроза1/Вразливіст2		
	Загроза2/Вразливість1		
	Загроза2/Вразливіст2		
	Загроза3/Вразливість1		
	Загроза3/Вразливіст2		

1. На основі отриманих даних зробити загальні висновки з виконаної роботи, а також визначити основні напрями удосконалення СЗІ об’єкта.

Завдання на виконання роботи:

1. До заданих інформаційних ресурсів та інформаційних потоків (заданих викладачем та визначених у попередній роботі) визначити перелік загроз (не менше 20).
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.

Лабораторна робота № 4

Тема: Розробка політики інформаційної безпеки

Мета роботи: Набуття досвіду зі створення політики інформаційної безпеки.

Кількість годин: 2 год.

Місце проведення: комп’ютерний клас.

Навчальні питання:

1. Види критеріїв в НД ТЗІ2.5-004-99.
2. Рівні кожної послуги.
3. Критерії гарантій середовища розробки.

Література:

1. Матеріали лекції 4.

[4, с. 13 – 28]

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.

Стислі теоретичні відомості

Політика інформаційної безпеки (ПІБ) є документом високого рівня, в якому описується мета, задачі та заходи щодо захисту інформації. ПІБ не являє собою ні директиву, ні норматив, ні інструкцію, ні засіб керування. Вона описує безпеку у загальних питаннях, не вдаючись у деталі. Тому ПІБ повинна охоплювати забезпечення усієї безпеки, аналогічно до того як специфікація визначає номенклатуру продукції, що випускається.

В процесі розробки ПІБ можуть виникнути потреба у технічній документації, однак сама технічна документація не повинна бути частиною ПІБ. Іншими словам ПІБ повинна вказувати на те що саме і від чого необхідно захищати, однак вона не передбачає як саме це буде здійснено, оскільки наявні засоби обчислювальної техніки на об’єкті захисту є швидкоплинними, якщо брати до уваги час, на який розробляється ПІБ, а відповідно швидкоплинними є і засоби захисту цих обчислювальних засобів. Аналогічні міркування стосуються і персоналу.

Перегляд ПІБ може обумовлюватись:

- зміною структури об’єкта захисту;
- зміною мети діяльності об’єкта захисту;
- виявленими проривами у системі захисту.

ПІБ не обов’язково повинна бути представлена єдиним документом, іноді допускається, щоб це був *комплекс* документів, які представлені як глави єдиної ПІБ. Наприклад, регламентація антивірусного захисту та розподіл доступу співробітників до ресурсів глобальних та локальних мереж можуть бути представлені різними документами, позаяк антивірусні засоби покликані забезпечити надійну та безпечну роботу користувачів локальних станцій, а

розмежування доступу вже стосується взаємодії одних локальних станцій з іншими. В будь-якому випадку ПІБ повинна бути повною та достатньою й підпорядковуватись низці певних класифікаційних критеріїв за якими можна переконатися у її повноті та достатності. Під повнотою розуміється охоплення всіх напрямів захисту, а під достатністю – те, що кожен з напрямів повинен передбачає захист від усіх загроз.

Кількість та обсяг документів істотно залежить від розміру, структури, мети діяльності (місії) об’єкта захисту.

Завдання на виконання роботи:

1. Вхідними даними роботи є критичні напрями захисту та основні небезпечні чинники, які студент має визначити відповідно до результатів виконання попередніх робіт. Вхідні дані коротко резюмувати у звіті.

2. Обґрунтувати вибір підходу до написання ПІБ, що розглянуті у стислих теоретичних відомостях (у вигляді єдиного документа або у вигляді комплексу документів).

3. Написати власне розділи ПІБ, які стосуються критичних напрямів. Розроблені розділи ПІБ повинні бути достатніми стосовно загроз перших трьох-п’яти рангів та передбачати правила захисту від загроз менших рангів.

4. Зробити загальні висновки з виконаної роботи, де визначити подальші дії щодо розробки повної ПІБ та кроки у випадку перегляду ПІБ внаслідок:

- поява (зникнення, якщо раніше був) відділу розробки спеціалізованого ПЗ для потреб об’єкта захисту (для студентів номер, яких за списком академічної групи кратний 3);
- зміни номенклатури виробництва (для студентів номер, яких за списком академічної групи при діленні на 3 має лишок 1);
- виникнення інциденту (для студентів номер, яких за списком академічної групи при діленні на 3 має лишок 2).

Лабораторна робота № 5

Тема : Дослідження моделі загроз (індивідуальне завдання)

Мета : Розглянути питання оцінки дій загроз в інформаційних системах

Кількість годин: 4 год.

Місце проведення: комп’ютерний клас.

Навчальні питання:

1. Вступ.
2. Види критеріїв в НД ТЗІ2.5-004-99.
3. Рівні кожної послуги.
4. Критерії гарантій середовища розробки.
5. Висновки.

Література:

1. Матеріали лекцій 2, 3.
   [2, 2 ч., с. 4 – 15]
   [3, 1 ч. с. 6 – 17]
   [3, 2 ч., с. 2 - 11]
   [3, 3 ч., с. 3 - 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.

Теоретичні відомості

Базові вимоги до побудови моделі загроз інформаційних систем.

Інформація є основною компонентою інформаційних систем різного призначення, в першу чергу автоматизованих систем з широким застосуванням засобів обчислювальної техніки. Разом з тим зростає частка інформації з обмеженим доступом, оскільки у сучасному світовому співтоваристві інформація набуває нового статусу, виступає в якості товару і по суті є гарантом успішної діяльності організації. Можна навести реальні факти, приклади, що саме цінність і вагомість інформації сприяє зростанню загроз, а саме викраденню, несанкціонованому використанню, знищенню інформації тощо. Тому актуальною проблемою по суті на інформаційній війні є створення методології, концепції захисту інформації в інформаційних системах, її облік, обробка і зберігання.

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 для аналізу одне з приміщень підприємства (кабінет директора, конференц зал тощо)

Виконати аналіз наявних в приміщенні типів технічних засобів, для цього використати таблицю наступного вигляду.

№ п.п	Тип технічного засобу	Покази	Технічні характеристики	Примітки (наявність підключення до локальної мережі чи мережі інтернету)
1	ПК			

Визначити можливі джерела знаття інформації.

Визначити за рахунок наявних технічних засобів у приміщенні можливі канали витоку інформації, для цього використати таблицю наступного вигляду.

№ п/п	Канали можливого витоку (знищення, спотворення) інформації	За рахунок чого
1	2	3

Оскільки для обробки ІзОД дозволено використовувати лише технічні засоби, які мають спеціальний на те дозвіл, виданий уповноваженою організацією, вважається що вони не створюють каналів витоку інформації (за умов їх правильного використання та відсутності можливості несанкціонованого доступу, що вирішується переважно організаційними заходами захисту, більш детальну інформацію можна знайти в таких документах НД ТЗІ 2.5-006-99, ТР ТЗІ - ПЕМВН-95, ТР ЕОТ-95, ДСТУ 3396.2-97 , ДСТУ 3396.2-97, ДСТУ 3396.2-97). В такому випадку такі технічні засоби розглядаються лише як джерело небезпечного впливу на допоміжні технічні засоби, не призначені для обробки ІзОД.

Наведіть види небезпечного впливу на допоміжні технічні засоби заповниши таблицю наведену нижче.

Основні технічні засоби та системи	Види небезпечного впливу на допоміжні технічні засоби
Технічні засоби обробки (перетворення) інформації в цілому	
Телефонні апарати	
Радіовипромінюючі засоби, в тому рахунку ПЕОМ.	
Лінійно-комутаційне обладнання зв’язку (кабелі, шафи, розподільчі пристрої, тощо)	

Навести рекомендації для підвищення рівня безпеки обраного для аналізу приміщення.

Лабораторна робота № 6

Тема: Складання техноробочого проекту створення КСЗІ (індивідуальне завдання).

Мета: Розглянути питання, щодо технорабочого проекту КСЗІ для інформаційної системи.

Кількість годин: 2 год.

Місце проведення: комп’ютерний клас.

Навчальні питання:

1. Відомість проектної документації до техноробочого проекту КСЗІ в АСВТЗІ.
2. Відомість експлуатаційної документації до техноробочого проекту КСЗІ в АСВТЗІ.
3. Основні технічні рішення та заходи при створенні КСЗІ в АСВТЗІ.
4. Висновки.

Література:

1. Матеріали лекції 1.

[1, 2 ч., с. 11 - 14]

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:

Оформити техноробочий проект щодо створення КСЗІ згідно індивідуального завдання.

Лабораторна робота № 7

Тема: Протокол випробувань комплексних систем захисту інформації

Мета роботи: Набуття досвіду зі створення документації систем захисту інформації.

Кількість годин: 4 год.

Місце проведення: комп'ютерний клас.

Навчальні питання:

1. Вступ.
2. Загальні відомості про протокол випробувань КСЗІ
3. НД ТЗІ 3.7-003-05
4. Зразок протоколу випробувань КСЗІ
5. Висновки.

Література:

1. Матеріали лекції 6.

[6, с. 11 – 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:

1. Дослідити структуру протоколу випробування КСЗІ.
2. Розробити протокол випробування КСЗІ для підприємства. Підприємство отримати у викладача або узяти з попередньої роботи згідно свого варіанту.

Лабораторна робота № 8

Тема: Документація на етапі експлуатації КСЗІ

Мета роботи: Набуття досвіду зі створення документації систем захисту інформації.

Кількість годин: 2 год.

Місце проведення: комп'ютерний клас.

Навчальні питання:

1. НД ТЗІ 2.6-001-11 – «Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах»

2. Зразок документації.
3. Висновки.

Література:

1. Матеріали лекції 6
[6, с. 11 – 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.

Теоретичні відомості

Документація ескізного проекту повинна містити основні проектні рішення щодо побудови КСЗІ (компонентів КСЗІ). Склад та зміст документації відповідно до ГОСТ 34.201-89 – «Інформаційна технологія. Види, комплектність та позначення документів при створенні автоматизованих систем», РД 50-34.698 – «Автоматизовані системи. Вимоги до змісту документів», в частині виготовлення конструкторської документації – стандартам ЕСКД (Єдина система конструкторської документації), в частині виготовлення програмної документації – стандартам ЕСПД, в частині виготовлення експлуатаційної документації – ГОСТ 34.201, РД 50-34.698-90. Документація відповідно до НД ТЗІ 2.5-004 – «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу».

На покупне ліцензійне програмне забезпечення та апаратні засоби надається документація, що входить до відповідних компонентів постачання програмного забезпечення та апаратури.

Перелік документів може уточнюватися у процесі розробки та реалізації проектних рішень упродовж всього етапу проектування. Обов’язковими є:

- детальний проект КСЗІ
- настанови адміністраторам
- настанови для користувачів

Експлуатаційна документація на КСЗІ повинна передаватися замовнику у вигляді копій на паперових та магнітних (оптичних) носіях.

НД ТЗІ 3.7-003-05 – «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомуніаційній системі».

Критерії оцінки захищеності інформації в комп’ютерній системі від НСД:

Склад обов'язкової проектної і експлуатаційної документації визначається вимогами нормативних документів, відповідно до яких проводиться розробка (зокрема, вимогами Критеріїв для відповідного рівня гарантій). Повний перелік необхідної документації визначається розробником КСЗІ і погоджується із замовником.

Для того, щоб замовник зміг повною мірою використати послуги безпеки, що надаються КС для реалізації політики безпеки, встановленої в його організації, йому необхідна відповідна документація, в якій були б описані ці послуги і дані вказівки щодо їх використання.

У складі експлуатаційної документації розробник повинен подати опис послуг безпеки, що реалізуються КЗЗ оцінюваної КС, настанови адміністратору щодо послуг безпеки і настанови користувачу щодо послуг безпеки. Зміст цих документів залежить від політики безпеки, що реалізується КС. Ніяких особливих вимог до назв, формату або структур документів дані критерії не ставлять.

Документація може бути загальною або в ній можуть бути явно виділені документи (розділи), призначені для адміністратора безпеки і для звичайного користувача. В будь-якому випадку наведеної в документації інформації повинно бути достатньо для того, щоб і адміністратор, і звичайні користувачі мали змогу виконувати свої функції.

Відповідно до НД ТЗІ 2.6-001-11 – «Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах» розглянемо наступні пункти:

А.2.2.2 Документація технічного проекту КСЗІ в ІТС

А.2.2.2.1 У документації технічного проекту КСЗІ, відповідно до положень НД ТЗІ 3.7-003-05, мають бути наведені відомості щодо загальних проектних рішень, достатніх (з урахуванням результатів ескізного проектування, зазначених у п. А.2.2.1) для забезпечення реалізації вимог

Технічного завдання на створення КСЗІ в ІТС, зазначеного в п. А.2.1.10 НД ТЗІ 2.6-001-11; рішень щодо структури КСЗІ (організаційної структури, структури технічних і програмних засобів); рішень щодо архітектури та складу КЗЗ КСЗІ (у тому числі щодо використовуваних засобів антивірусного захисту, засобів виявлення та попередження про мережеві вторгнення тощо); рішень щодо механізмів реалізації ФПБ, визначених у наведеному в Технічному завданні функціональному профілі захищеності; рішень щодо алгоритмів, порядку та умов функціонування засобів захисту інформації, які використовуються у складі КЗЗ КСЗІ для реалізації певних ФПБ (функцій захисту).

А.2.2.2.2 Зміст та склад документації технічного проекту повинні бути достатніми для повного опису проектних рішень КСЗІ в обсязі, достатньому для виконання етапу робочого (технороботочого) проектування (реалізації) КСЗІ. Конкретний перелік документації технічного проекту має визначатися на підставі ГОСТ 34.201-89 та РД 50-34.698-90 з урахуванням особливостей відповідної КСЗІ. Обов'язковою є наявність пояснювальної записки до технічногопроекту КСЗІ, структура та зміст якої повинні відповідати вимогам РД 50-34.698-90 та рекомендаціям НД ТЗІ 2.7-010-09 –« Методичні вказівки з оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу» (у частині, що стосується проекту

архітектури та детального проекту компонентів КЗЗ КСЗІ, створення яких здійснюється в ході створення КСЗІ, для визначеного у Технічному завданні на створення КСЗІ в ІТС рівня гарантій коректності реалізації ФПБ).

А.2.2.2.3 Документація технічного проекту КСЗІ в ІТС має бути погоджена з Розробником ІТС, затверджена виконавцем робіт зі створення КСЗІ в ІТС та керівником (заступником керівника) організації (установи), яка є власником (розпорядником) ІТС.

А.2.5 Експлуатаційна документація компонентів (складових частин) КЗЗ КСЗІ

А.2.5.1 До складу експлуатаційної документації мають входити документи, що визначають порядок інсталяції, ініціалізації, налаштування та експлуатації всіх без винятку компонентів (складових частин) КЗЗ КСЗІ, визначених у документації технічного проекту КСЗІ в ІТС, зазначеній у п.А.2.2.2.

А.2.5.2 Відповідно до вимог НД ТЗІ 2.5-004-99, для кожного компонента (складової частини) КЗЗ КСЗІ у вигляді окремих документів або розділів інших документів повинні бути надані:

- опис процедур безпечної інсталяції, генерації та запуску;
- опис послуг безпеки, що реалізуються відповідним компонентом;
- настанови адміністратору з послуг безпеки;
- настанови користувачу з послуг безпеки.

А.2.5.3 Зміст відповідних документів повинен відповідати вимогам НД ТЗІ 2.5-004-99 та рекомендаціям НД ТЗІ 2.7-010-09.

Створюється пакет документів «Експлуатаційна документація на КСЗІ», який включає: - Інструкції експлуатації КСЗІ та її елементів; - Процедури регламентного обслуговування КСЗІ; - Правила та положення з проведення тестування і аналізу роботи КСЗІ.

Відповідно до НД 3.7.003-05

6.5.6.4 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.

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

6.5.7 Дослідна експлуатація

6.5.7.1 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.

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

Завдання на виконання роботи:

Сформуйте настанови:

а) адміністратору;

б) користувачу;

2) інструкції експлуатації КСЗІ та її елементів;

Лабораторна робота № 9

Тема: Програма та методика попередніх випробувань комплексної системи захисту інформації»

Мета: практичне ознайомлення з програмою та методикою попередніх випробувань КСЗІ в ІТС.

Кількість годин: 2 год.

Місце проведення: комп’ютерний клас.

Навчальні питання:

1. НД ТЗІ 3.7-003-2005 Методика попередніх випробувань КСЗІ
2. Зразок документації.
3. Висновки.

Література:

1. Матеріали лекцій 1, 6.

[3 ч. 3 с. 8 – 11]
[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:

1. Розробити згідно НД ТЗІ 3.7-003-05 методику попередніх випробувань для 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/