Міністерство освіти і науки України

Національний університет водного господарства
та природокористування

Кафедра обчислювальної техніки

04-04-212

МЕТОДИЧНІ ВКАЗІВКИ

до лабораторних робіт із навчальної дисципліни
"Організація захисту інформації в комп'ютерних системах"
для здобувищої освіти другого (магістерського) рівня
за спеціальністю 123 "Комп'ютерна інженерія"
денної та заочної форм навчання

Рекомендовано науково-методичною
комісією зі спеціальності 123
"Комп'ютерна інженерія"
протокол № 1 від 08.09.2018 р.

Рівне – 2018

Методичні вказівки до лабораторних робіт із навчальної дисципліни "Організація захисту інформації в комп'ютерних системах" для здобувачів вищої освіти другого (магістерського) рівня галузі знань 12 "Інформаційні технології" за спеціальністю 123 "Комп'ютерна інженерія" спеціалізації «Комп'ютерні системи та компоненти» денної та заочної форм навчання / Назарук В. Д. – Рівне : НУВГП. – 60 с.

Укладач: В. Д. Назарук, кандидат технічних наук, старший викладач кафедри обчислювальної техніки.

Відповідальний за випуск – Б. Б.Круліковський, завідувач кафедри обчислювальної техніки.

ЗМІСТ

Вступ

Інформаційні ресурси держави або суспільства загалом, а також окремих організацій і фізичних осіб є певною цінністю, мають відповідне матеріальне вираження і потребують захисту від різноманітних впливів, що можуть спричинити зниження цінності інформаційних ресурсів. Передусім це стосується загроз і впливів на інформацію, що обробляється, зберігається та передається за допомогою комп'ютерних систем.

Для належного захисту інформаційних ресурсів слід вирішити такі завдання:

- визначити вимоги щодо захисту комп'ютерних систем від несанкціонованого доступу;

- створити захищені комп'ютерні системи і засоби їх захисту від несанкціонованого доступу;

- оцінити захищеність комп'ютерних систем і їх придатність для вирішення завдань споживача.

Методологічні основи (концепцію) вирішення завдань захисту інформації в комп'ютерних системах визначено в нормативних і методологічних документах, регламентуючих питання технічного захисту інформації.

Під час створення комплексних систем захисту інформації використання нормативних документів із питань технічного захисту інформації (НД ТЗІ) є обов'язковим. Тому практичне застосування вимог НД ТЗІ в процесі вивчення навчальної дисципліни «Організація захисту інформації» має важливе значення і викладено як лабораторний практикум.

Методичні вказівки до лабораторних робіт дають студентам змогу набути навиків створення комплексних систем захисту інформації та підготовки супровідних документів.

Пропоновані методичні вказівки можуть бути корисні фахівцям установ, підприємств та організацій, що займаються

створенням і супроводженням комплексних систем захисту інформації.

Загальні методичні вказівки

Лабораторні роботи спрямовані на відпрацювання студентами вмінь і навиків використання чинних нормативних документів у галузі технічного захисту інформації для створення комплексних систем захисту інформації (КСЗІ).

Як умовний зразок комп'ютерної системи, для якої необхідно створювати КСЗІ, обирають автоматизовану систему класу 1 (АС класу 1), встановлену **в підрозділі кадрового забезпечення організації** (установи, підприємства), де студент працює, працював, або проходив практику. АС призначена для обробки інформації з обмеженим доступом, що містить персональні дані співробітників організації.

Під час виконання лабораторних робіт використовують та конкретизують положення НД ТЗІ, які відповідають вимогам і умовам, притаманним для вищевказаної організації (АС).

Кожна лабораторна робота розрахована на 2 години лабораторних занять.

Звіти про кожну лабораторну роботу виконують у текстовому редакторі Word, зберігають окремим документом і надсилають на перевірку викладачу.

Лабораторна робота №1
Застосування термінів, визначених нормативними документами ТЗІ для підготовки документів при створенні КСЗІ

Завдання лабораторної роботи:

1.1. Ознайомитися із термінами і визначеннями понять у галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу, обов'язковими для застосування в усіх видах документації і літератури, що входять до системи технічного захисту інформації. Терміни і визначення викладено в НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу»

1.2. Відповідно до варіанта, який співпадає з номером за списком в групі (табл. 1.1) підготувати визначення десяти термінів і понять, які в обов'язковому порядку застосовуються в усіх видах документів системи технічного захисту інформації. Необхідно також привести еквіваленти їх термінів у міжнародних стандартах.

Таблиця 1.1

Варіанти вибору термінів

№ студ. в групі	№ завдання									
	1	2	3	4	5	6	7	8	9	10
1	4.1.1	4.1.3	4.1.5	4.1.7	4.1.9	4.1.11	4.1.13	4.1.15	4.1.17	4.1.19
2	4.1.21	4.1.23	4.1.25	4.1.27	4.1.29	4.1.31	4.1.33	4.2.1	4.2.3	4.2.5
3	4.2.7	4.2.9	4.2.11	4.2.13	4.2.15	4.2.17	4.2.19	4.2.21	4.2.23	4.2.25
4	4.2.	4.3.	4.3.	4.3.	4.3.	4.3.	4.3.	4.3.	4.3.	4.3.

	27	2	4	6	8	10	12	14	16	18
5	4.3.20	4.3.22	4.4.2	4.4.4	4.4.6	4.4.8	4.4.10	4.4.12	4.4.14	4.4.16
6	4.4.18	4.4.20	4.4.22	4.4.24	4.4.26	4.4.28	4.4.30	4.4.32	4.4.34	4.4.36
7	4.4.38	4.4.40	4.4.42	4.4.44	4.1.1	4.1.3	4.1.5	4.1.7	4.1.9	4.1.11
8	4.1.31	4.1.33	4.2.1	4.2.3	4.2.5	4.1.21	4.1.23	4.1.25	4.1.27	4.1.29
9	4.4.8	4.4.10	4.4.12	4.4.14	4.4.16	4.2.7	4.2.9	4.2.11	4.2.13	4.2.15
10	4.4.28	4.4.30	4.4.32	4.4.34	4.4.36	4.2.27	4.3.2	4.3.4	4.3.6	4.3.8
11	4.1.2	4.1.4	4.1.6	4.1.8	4.1.10	4.1.12	4.1.14	4.1.16	4.1.18	4.1.20
12	4.1.22	4.1.24	4.1.26	4.1.28	4.1.30	4.1.32	4.1.34	4.2.2	4.2.4	4.2.6
13	4.2.8	4.2.10	4.2.12	4.2.14	4.2.16	4.2.18	4.2.20	4.2.22	4.2.24	4.2.26
14	4.3.1	4.3.3	4.3.5	4.3.7	4.3.9	4.3.11	4.3.13	4.3.15	4.3.17	4.3.19
15	4.3.21	4.4.1	4.4.3	4.4.5	4.4.7	4.4.9	4.4.11	4.4.13	4.4.15	4.4.17
16	4.4.19	4.4.21	4.4.23	4.4.25	4.4.27	4.4.29	4.4.31	4.4.33	4.4.35	4.4.37
17	4.4.39	4.4.41	4.4.43	4.4.45	4.1.2	4.1.4	4.1.6	4.1.8	4.1.10	4.1.12
18	4.1.32	4.1.34	4.2.2	4.2.4	4.2.6	4.1.22	4.1.24	4.1.26	4.1.28	4.1.30
19	4.4.9	4.4.11	4.4.13	4.4.15	4.4.17	4.2.8	4.2.10	4.2.12	4.2.14	4.4.6
20	4.4.	4.4.	4.4.	4.4.	4.4.	4.3.	4.3.	4.3.	4.3.	4.4.

	29	31	33	35	37	1	3	5	7	26

1.3. Отримані результати занести в звіт як у табл. 1.2.

Таблиця 1.2.

Термінологія в галузі ТЗІ (10 термінів)

№ з/п	Пункт НД ТЗІ	Термін	Визначення	Еквіваленти термінів міжнародних стандартів
1	*4.1.1*	*Обчислювальна система*	*Сукупність програмних-апаратних засобів, призначених для обробки інформації*	*computer system*
2				

Лабораторна робота № 2
Підготовка Загальних положень та розділу 1 «Положення про службу захисту інформації»

Завдання лабораторної роботи:

2.1. Ознайомитися з вимогами розділів 1-7 НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі».

2.2. Застосовуючи положення та вимоги, викладені в розділах 6, 7 зазначеного нормативного документу, розробити розділи «Загальні положення», та «Розділ 1. Завдання служби захисту інформації», які повинні входити до «Положення про службу захисту інформації» для АС, зазначеної у вступі лабораторного практикуму.

2.3. Звіт про виконання лабораторної роботи подати у вигляді одного документу, в який входять наступні розділи:

- «Загальні положення»;
- «Розділ 1. Завдання служби захисту інформації».

Лабораторна робота № 3
Підготовка розділу 2 «Положення про службу захисту інформації»

Завдання лабораторної роботи:

3.1. Ознайомитися з вимогами розділу 8 НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі».

3.2. Застосовуючи положення та вимоги, викладені в розділі 8 зазначеного нормативного документу, розробити «Розділ 2. Функції служби захисту інформації», в який входять підрозділи «2.1. Функції під час створення комплексної системи захисту інформації», «2.2. Функції під час експлуатації комплексної системи захисту інформації», «2.3. Функції з організації навчання персоналу щодо забезпечення захисту інформації», які повинні входити до «Положення про службу захисту інформації» для АС, зазначеної у вступі лабораторного практикуму.

3.3. Звіт про виконання лабораторної роботи подати у вигляді одного документу «Розділ 2. Функції служби захисту інформації», в який входять наступні підрозділи:

- 2.1. Функції під час створення комплексної системи захисту інформації;
- 2.2. Функції під час експлуатації комплексної системи захисту інформації;
- 2.3. Функції з організації навчання персоналу з питань забезпечення захисту інформації.

Лабораторна робота № 4
Підготовка розділу 3 «Положення про службу захисту інформації».

Завдання лабораторної роботи:

4.1. Ознайомитись з вимогами розділу 9 НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі».

4.2. Застосовуючи положення та вимоги, викладені в розділі 9 зазначеного нормативного документа, розробити «Розділ 3. Повноваження та відповідальність служби захисту інформації», що містить підрозділи «3.1. Права», «3.2. Обов'язки», «3.3. Відповідальність», які повинні входити до «Положення про службу захисту інформації» для АС, зазначеної у вступі лабораторного практикуму.

4.3. Звіт про виконання лабораторної роботи подати як один документ «Розділ 3. Повноваження та відповідальність служби захисту інформації», що містить такі підрозділи:

- 3.1. Права;
- 3.2. Обов'язки;
- 3.3. Відповідальність.

Лабораторна робота № 5
Підготовка розділів 4 – 5 «Положення про службу захисту інформації».

Завдання лабораторної роботи:

5.1. Ознайомитися з вимогами розділів 9 – 11 НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі».

5.2. Застосовуючи положення та вимоги, викладені в розділі 8 зазначеного нормативного документу, розробити: «Розділ 4. Взаємодія служби захисту інформації з іншими підрозділами організації та зовнішніми організаціями», «Розділ 5. Штатний розклад та структура служби захисту інформації», «Розділ 6. Фінансування служби захисту інформації», які повинні входити до «Положення про службу захисту інформації» для АС, зазначеної у вступі лабораторного практикуму.

5.3. Звіт про виконання лабораторної роботи подати у вигляді одного документу, в який входять наступні розділи:

5.1. Розділ 4. Взаємодія служби захисту інформації з іншими підрозділами організації та зовнішніми організаціями;

5.2. Розділ 5. Штатний розклад та структура служби захисту інформації;

5.3. Розділ 6. Фінансування служби захисту інформації.

Лабораторна робота № 6
Підготовка розділів 1,2 «Плану захисту інформації в автоматизованій системі»

Завдання лабораторної роботи:

6.1. Ознайомитися з вимогами вступу та розділів 1,2 додатку «План захисту інформації в автоматизованій системі» до НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі».

6.2. Застосовуючи положення та вимоги, викладені у вступі та розділах 1,2 зазначеного додатку, розробити: «Розділ 1. Завдання захисту інформації в АС», та «Розділ 2. Класифікація інформації, що обробляється в АС», які повинні входити до «Плану захисту інформації в автоматизованій системі» для АС зазначеної у вступі лабораторного практикуму.

Розділ 2. «Класифікація інформації, що обробляється в АС» виконується за наступним зразком.

Зразок

У приміщенні № __ функціонує 1 автоматизована система, що належить до АС класу __ категорії. За правовим режимом інформація, яку обробляють в АС поділена на інформацію з обмеженим доступом (ІзОД), що містить персональні дані та відкриту інформацію.

Порядок доступу до ІзОД, що циркулює в АС, наступний.

1. Відповідальність за забезпечення режиму обробки ІзОД при використанні АС, своєчасне розроблення, впровадження та організацію виконання відповідних режимних заходів, покладається на керівництво (назва підприємства), адміністратора безпеки та безпосередньо на користувачів АС.

2. Користувачам заборонено змінювати права доступу до інформації в АС.

3. Доступ до виконання робіт на автоматизованих системах, призначених для обробки ІзОД, отримують тільки за умови службової необхідності співробітники, які мають оформлений в установленому порядку допуск до ІзОД, практичні навички роботи на ПЕОМ і затверджені наказом керівництва (назва підприємства) користувачі АС.

4. Під час обробки ІзОД в автоматизованих системах ЗАБОРОНЯЄТЬСЯ:

- *обробляти інформацію з грифом вище, ніж визначено актом категоріювання цього об'єкта ЕОТ;*
- *обробляти ІзОД у присутності осіб, які не мають до неї відношення;*
- *при обробці ІзОД виконувати іншу, не пов'язану з цим роботу;*
- *використовувати ПЕОМ поза призначенням;*
- *записувати ІзОД на незареєстровані машинні носії даних;*
- *вносити несанкціоновані схемні і конструктивні зміни в ПЕОМ;*
- *використовувати для обробки ІзОД недозволене програмне забезпечення;*
- *допускати до будь-яких робіт на ПЕОМ осіб, які не внесені до переліку користувачів даної системи;*
- *виконувати будь-які інші дії, що можуть призвести до втрати або розголошення ІзОД.*

5. Облік магнітних носіїв даних, паперових документів і документів в електронному вигляді, підготовлених з використанням ПЕОМ, організовується і ведеться відділом_____ (назва підприємства).

6. ІзОД повинна зберігатися тільки на облікованих МНД, які мають відповідний ступінь обмеження доступу. У разі виявлення факту зберігання на не облікованих МНД

інформації з обмеженим доступом, ці МНД підлягають негайному взяттю на облік у встановленому порядку та проводиться службове розслідування.

7. ІзОД у процесі обробки в АС не повинна підлягати неконтрольованому та несанкціонованому ознайомленню, розмноженню, розповсюдженню, копіюванню, відновленню, а також неконтрольованій та несанкціонованій модифікації.

8. МНД, що використовують для обміну інформацією між співробітниками (або підрозділами), повинні містити тільки ту інформацію, яка необхідна для передачі.

9. Друкують документи, що містять ІзОД, на принтерах в АС класу "1" лише співробітники, які мають право роботи на цій АС.

10. Після виконання документу на ПЕОМ його потрібно негайно зареєструвати в відділі _____ (назва підприємства), при цьому на документі виставити всі необхідні реквізити.

6.3. Звіт про виконання лабораторної роботи подати у вигляді одного документу, в який входять наступні розділи:

1. Розділ 1. Завдання захисту інформації в АС;
2. Розділ 2. Класифікація інформації, що обробляється в АС.

Лабораторна робота № 7
Підготовка розділу 3 «Плану захисту інформації в автоматизованій системі»

Завдання лабораторної роботи:

7.1. Ознайомитись з вимогами розділу 3 додатку «План захисту інформації в автоматизованій системі» до НД ТЗІ 1.4-

001-2000 «Типове положення про службу захисту інформації в автоматизованій системі».

7.2. Застосовуючи положення та вимоги, викладені в розділі 3 зазначеного додатку, розробити: «Розділ 3. Опис компонентів АС та технології обробки інформації» який повинен входити до «Плану захисту інформації в автоматизованій системі» для АС, зазначеної у вступі лабораторного практикуму.

7.2.1. Розділ 3. «Опис компонентів АС та технології обробки інформації» виконується за нижченаведеним зразком.

Зразок

Склад технічних засобів АС, визначених під час інвентаризації наведено в табл. 3.1

Таблиця 3.1

Склад технічних засобів АС_____(назва підприємства)

№ з/п	*Пристрій*	*Тип*	*№*
1	*Корпус системного блоку*		
2	*HDD*		
3	*Блок живлення*		
4	*Материнська плата*		
5	*Процесор*		
6	*Маніпулятор «мишка»*		
7	*DWD-RW*		
8	*Клавіатура*		
9	*Монітор*		
10	*Принтер*		
11	*Флеш-*		

	накопичувачі		
12	*Інші наявні пристрої*		

3.2. Опис програмного забезпечення АС _____(назва підприємства)

- *операційна система: (Windows …, Linux):*
- *драйвери:*
- *утиліти, архіватори: WinRar, WinZip;*
- *антивіруси: Avast, …;*
- *програми для діагностики комп'ютера:*
- *програми дефрагментації дисків;*
- *програми для оптимізації дисків:*
- *програми-оболонки: (FAR, Win32, Nc, Dn);*
- *офісна програма: Microsoft Office - ….*
- *інші:*

3.3. Дані

В АС ___ (назва підприємства) впроваджено технології обробки інформації, що потребує захисту, тобто способи і методи застосування засобів обчислювальної техніки під час виконання функцій збору, зберігання, обробки, передачі і використання даних.

За способом реалізації процедури розмежування доступу до ІЗОД та технології її обробки, що можуть бути запроваджені в АС класу «1», наступні:

- *дані ІЗОД у вигляді файлів різних форматів зберігаються на з'ємних та нез'ємних магнітних, оптичних та флеш носіях інформації;*
- *користувачі мають різні повноваження стосовно доступу до даних ІЗОД, які розміщені на носії інформації;*

- *на носіях інформації зберігаються дані різних ступенів обмеження;*
- *ступінь обмеження носія інформації повинен відповідати вищому ступеню обмеження даних, які на ньому зберігаються.*

Надійним засобом гарантування цілісності інформаційних масивів і системних програмних засобів від ураження комп'ютерними вірусами є використання користувачами ПЕОМ певних правил, до яких можна віднести:

- *обов'язкове регулярне резервне копіювання системних програмних засобів та важливої інформації, що забезпечує можливість її швидкого відновлення від вірусів або вірусних атак;*
- *отримання програмного забезпечення встановленим порядком;*
- *перевірка перед використанням всіх машинних носіїв даних;*
- *визначення кола користувачів, допущених до роботи на конкретному комп'ютері та ознайомлення їх з порядком застосування антивірусних програмних засобів.*

3.4. Користувачі

До роботи в АС можуть бути допущені наступні категорії користувачів:

- *Користувачі (підрозділу, в якому встановлена АС:(посади);*
- *Користувачі, які мають повноваження адміністраторів АС:(посади);*
- *Користувачі, які мають повноваження керувати засобами КСЗ:(посади);*
- *Користувачі контролюючих організацій.*

7.3. Звіт про виконання лабораторної роботи подати у вигляді документу, в який входить один розділ:

1. Розділ 3. Опис компонентів АС та технології обробки інформації;

Лабораторна робота № 8
Підготовка підрозділу 4.1. розділу 4. «Плану захисту інформації в автоматизованій системі»

Завдання лабораторної роботи:

8.1. Ознайомитися з вимогами розділу 4 додатку «План захисту інформації в автоматизованій системі» до НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі».

8.2. Розділ 4. «Загрози для інформації в АС» повинен складатись із двох підрозділів:

- 4.1. Модель загроз;
- 4.2 Модель порушника.

8.3. Застосовуючи положення та вимоги, викладені в розділі 4 зазначеного додатку, розробити підрозділ 4.1. «Модель загроз» Розділу 4. «Загрози для інформації в АС», який повинні входити до «Плану захисту інформації» в АС, зазначеній у вступі лабораторного практикуму.

8.4. Під час застосування положень п.4.2.1 Додатку необхідно враховувати, що при відсутності обробки в АС секретної інформації загрози, спричинені технічними каналами, що включають канали побічних електромагнітних випромінювань і наводок, акустичними, оптичними, радіо- та радіотехнічними, хімічними та іншими каналами а також каналами спеціального впливу шляхом формування полів і сигналів враховувати не обов’язково.

8.5. Підрозділ 4.1. «Модель загроз» Розділу 4. «Загрози для інформації в АС» виконують за нижченаведеним зразком.

Зразок

4.1. Модель загроз

Перелік суттєвих загроз та методи і способи їхнього здійснення.

Існують наступні загрози для інформації, що обробляється та накопичується в АС:

- *несанкціонований фізичний доступ до технічних засобів АС;*
- *здійснення НСД до ІзОД, що обробляється в АС, шляхом порушенням встановлених правил управління доступом до ІзОД;*
- *помилки у ПЗ та відмови (збої) у функціонуванні ПЗ та технічних засобів АС;*
- *впровадження комп'ютерних вірусів та закладних програм;*
- *неправильні дії персоналу;*
- *надзвичайні ситуації.*

4.1.1. Несанкціонований фізичний доступ до технічних засобів.

Несанкціонований фізичний доступ до технічних засобів АС може реалізовуватися шляхом проникнення порушника у приміщення, де такі засоби розташовано. У випадку реалізації цієї загрози створюються передумови для порушення цілісності, конфіденційності і доступності інформації.

Заходи та засоби протидії:

- визначення порядку фізичного доступу співробітників та відвідувачів у приміщення, де розташовані АС (шляхом затвердження переліків осіб, яким дозволено знаходитись у приміщенні);

- розробка та додержання регламенту розкриття та опечатування приміщень, постановки та зняття їх з охоронної сигналізації;

- забезпечення охорони приміщень, де розташовані АС у неробочий час;

- регламентування порядку дій персоналу та охорони у випадку реалізації спроб несанкціонованого фізичного доступу.

4.1.2. Здійснення НСД до ІзОД, що обробляється в АС шляхом порушенням встановлених правил управління доступом до ІзОД.

Несанкціонований доступ до інформації здійснюється з порушенням встановлених в АС правил управління доступом, а саме підключення порушника до системи під ідентифікатором або паролем зареєстрованого користувача з подальшим використанням недозволеного програмного забезпечення для отримання доступу до інформаційних ресурсів в обхід системи управління доступом КСЗІ. У випадку реалізації цієї загрози створюються передумови для порушення цілісності, конфіденційності і доступності інформації.

Заходи та засоби протидії:

- надання користувачам права доступу, що не дозволяють встановлювати ПЗ;

- реєстрація дій користувачів у захищеному журналі аудиту.

4.1.3. Помилки у ПЗ та відмови (збої) у функціонуванні ПЗ та технічних засобів АС.

Порушення функціонування ПЗ та технічних засобів АС відбуваються через помилки, які робляться на етапі

встановлення ПЗ, а також через відмову працездатності технічних засобів АС. У цьому випадку існує загроза щодо порушення цілісності, конфіденційності і доступності інформації.

Заходи та засоби протидії:

- забезпечення заданого рівня критеріїв гарантій до ПЗ АС;

- створення резервних копій ПЗ та інформаційних фондів;

- планування та проведення регламентних робіт щодо технічних засобів АС;

- створення фонду запасних технічних засобів.

4.1.4. Ураження комп'ютерними вірусами та впровадження закладних програм.

Ураження комп'ютерними вірусами та впровадження закладних програм може бути наслідком, як реалізації загрози НСД, так і неправильних дій персоналу, а саме застосування несанкціонованого ПЗ. У цьому випадку створюються передумови для порушення цілісності, конфіденційності і доступності інформації.

4.1.5. Неправильні дії персоналу.

Неправильні дії персоналу трапляються внаслідок його низької кваліфікації, недбалого ставлення до своїх службових обов'язків або свідомого завдання шкоди. У випадку реалізації цієї загрози створюються передумови для порушення цілісності, конфіденційності і доступності інформації.

Внаслідок таких дій персоналу можуть трапитись:

- відмови окремих компонентів, руйнування технічних засобів АС, програмних ресурсів (обладнання, каналів зв'язку, втрата даних, програм та ін.);

- ненавмисне пошкодження носіїв інформації;

- неправомірна зміна режимів роботи АС (окремих компонентів, обладнання, ПЗ тощо), ініціювання тестуючих або технологічних процесів, які здатні призвести до незворотних змін у системі (наприклад, форматування носіїв інформації або знищення окремих інформаційних ресурсів);

- ненавмисне зараження ПЗ комп'ютерними вірусами;

- неконтрольоване поширення інформації з АС, паролів та ідентифікаторів користувачів, іншої інформації щодо режимів роботи АС;

- неправомірне впровадження і використання стороннього ПЗ (наприклад, навчальних та ігрових програм, несанкціонованого системного і прикладного ПЗ та ін.).

Заходи та засоби протидії:

- *організація професійної підготовки;*
- *моделювання неправильних дій персоналу;*
- *ведення журналів аудиту дій користувачів у АС;*
- *регламентація порядку допуску користувачів до роботи з АС.*

4.1.6. Надзвичайні події.

Надзвичайні події (пожежа, затоплення, землетрус, виникнення радіаційної та хімічної небезпеки) можуть бути причиною порушення конфіденційності, цілісності і доступності інформації.

Заходи та засоби протидії:

- *проведення учбових занять з користувачами АС щодо їх дій на випадок виникнення надзвичайних ситуацій;*
- *організація системи сповіщення;*
- *впровадження технічних засобів протидії (мінімізації шкоди) від загрози, які включають протипожежне обладнання, систему сповіщення персоналу, резервного електропостачання;*
- *створення запасних комплектів технічних засобів,*

резервних копій ПЗ та інформаційних ресурсів АС.

Модель загроз безпеки інформації в автоматизованій системі класу «1» формалізовано представлено в табл.4.1 «Перелік загроз інформації», де використовуються наступні скорочення для позначення тих характеристик інформації, на які впливає та або інша загроза: К - конфіденційність, Ц – цілісність, Д - доступність, С - спостереженість. В стовпцях графи «Наслідки» знаком «+» відмічається можливість виникнення зазначеної загрози.

Табл. 4.1

Перелік загроз інформації

№ з/п	*Тип та визначення загроз*	*Джерело загроз*	*Наслідки*			
			К	*Ц*	*Д*	*С*
1	*Пожежа, повінь, землетрус, ураган, вибух*	*Середовище*		+	+	
2	*Вологість, запиленість, зміни температури*	*Середовище*		+	+	
Випадкові загрози технічного походження						
3	*Аварія системи життєзабезпечення*	*Середовище*				
4	*Відмови (повний вихід з ладу, систематичне неправильне виконання своїх функцій) людей*	*Людина*				
5	*Відмови основної*	*Апаратура*				

	апаратури, систем передавання даних, носіїв інформації					
6	*Відмови програмного забезпечення*	*Програмне забезпечення*				
7	*Відмови системи живлення, систем забезпечення нормальних умов роботи апаратури та персоналу (електроживлення, охолодження та вентиляції, ліній зв'язку тощо)*	*Середовище, апаратура*				
8	*Збої систем живлення, систем забезпечення нормальних умов роботи апаратури та персоналу*	*Середовище, апаратура*				
9	*Випадкові помилки користувачів, обслуговуючого персоналу, помилкове конфігурування та адміністрування системи*	*Людина*				
10	*Недбале зберігання та облік документів та носіїв інформації*	*Людина*				
11	*Помилка апаратури*	*Людина*				
12	*Пошкодження носіїв*	*Людина,*				

	інформації	*апаратура*				
13	*Ураження програмного забезпечення комп'ютерними вірусами*	*Людина, програмне забезпечення*				
Навмисні загрози техногенного походження контактної дії						
14	*Читання «сміття» (залишкової інформації з запам'ятовуючих пристроїв)*	*Апаратура, програмне забезпечені, Людина*				
15	*Оглядання даних, що виводяться на екран*	*Людина, апаратура*				
16	*Оглядання даних, що роздруковуються, читання без догляду віддрукованих на принтері документів*	*Людина, апаратура*				
17	*Відключення або вивід з ладу підсистем забезпечення функціонування обчислювальних систем (електроживлення, охолодження та вентиляції, ліній зв'язку тощо)*	*Людина, апаратура, програмне забезпечення*				
18	*Фізичне зруйнування системи (внаслідок вибуху, підпалення*	*Людина*				

	тощо) пошкодження всіх або окремих найбільш важливих компонентів АС (пристроїв, носіїв важливої інформації, осіб з числа персоналу тощо), систем електроживлення тощо					
19	*Провокування до розмов осіб, що мають відношення до АС*	*Людина*				
20	*Копіювання вихідних документів, магнітних то інших носіїв інформації (у тому числі при проведенні ремонтних та регламентних робіт)*	*Апаратура, програмне людина*				
21	*Розкрадання магнітних носіїв та документів (оригінали і копії інформаційних матеріалів, ГМД), виробничих відходів (відбитків, записів, носіїв інформації тощо), отримання необлікованих копій*	*Людина*				
22	*Незаконне отримання паролів та інших*	*Людина, програмне*				

	реквізитів розмежування доступу (агентурним шляхом, внаслідок недбалості користувачів, підбором імітацією інтерфейсу системи тощо) з наступним маскуванням під зареєстрованого користувача («маскарад»)	*забезпечення*				
23	*Несанкціоноване використання технічних пристроїв (принтер та інші периферійні пристрої)*	*Людина, програмне забезпечення*				
24	*Обхід механізмів захисту з метою забезпечити в подальшому несанкціонований доступ порушника*	*Людина, програмне забезпечення*				
25	*Перехоплення паролів програмою-імітатором, включення в програми програмних закладок типу «троянський кінь», «бомба» тощо*	*Людина, програмне забезпечення*				
26	*Використання «вад»*	*Людина,*				

	мов програмування, операційних систем (у тому числі параметрів системи захисту, встановлених «за умовчанням»)	*програмне забезпечення*				
27	*Несанкціоновані зміни, підміна елементів програм елементів баз даних, апаратури, магнітних носіїв*	*Людина, програмне забезпечення*				

8.6. Звіт про виконання лабораторної роботи подати у вигляді документу, в який входить один підрозділ:

4.1. Модель загроз

Лабораторна робота № 9

Підготовка підрозділу 4.2. розділу 4. «Плану захисту інформації в автоматизованій системі»

Завдання лабораторної роботи:

9.1. Ознайомитися з вимогами розділу 4 додатку **«**План захисту інформації в автоматизованій системі**»** до НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі».

9.2. Розділ 4. «Загрози для інформації в АС» повинен складатись із двох підрозділів:

- 4.1. Модель загроз;
- 4.2 Модель порушника

9.3. Застосовуючи положення та вимоги, викладені в розділі 4 зазначеного додатку, розробити підрозділ 4.2 «Модель порушника» Розділу 4 «Загрози для інформації в АС», який

повинні входити до «Плану захисту інформації» в АС, зазначеній у вступі лабораторного практикуму.

9.4. Під час застосування положень п.4.2.1 Додатку слід враховувати, що при відсутності обробки в АС секретної інформації загрози, спричинені технічними каналами, що включають канали побічних електромагнітних випромінювань і наводок, акустичними, оптичними, радіо- та радіотехнічними, хімічними та іншими каналами а також каналами спеціального впливу шляхом формування полів і сигналів враховувати не обов'язково.

9.5. Підрозділ 4.2. «Модель порушника» Розділу 4. «Загрози для інформації в АС» виконується за нижченаведеним зразком.

Зразок

4.2. Модель порушника

Порушник – це особа, яка помилково, через необізнаність, цілеспрямовано, за злим умислом або без нього, використовуючи різні можливості, методи й засоби, зробила спробу виконати операції, які спричинили або можуть спричинити порушення захищеності інформації.

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

Порушники можуть бути внутрішніми (з числа персоналу/користувачів АС), або зовнішніми (з числа сторонніх осіб). Зовнішні порушники у даних умовах можуть бути з числа представників організацій, що взаємодіють з питань технічного забезпечення (енерго, водо, теплопостачання, співробітники сервісних центрів тощо) і внаслідок чого мають доступ на територію розташування АС, і діють на цій території чи за її межами, або з числа осіб, які зацікавлені в

порушенні робот АС, але доступу у контрольовану зону не мають.

На модель порушника впливають такі факти:

- розташування адмінбудинку, в якому розміщено АС, на території, яка має систему надійної фізичної охорони, що практично виключає неконтрольоване проникнення у приміщення сторонніх осіб;

- ретельний підбір співробітників на відповідні посади, що практично виключає виконання ключових функціональних ролей "випадковими" особами; усі співробітники, що задіяні на таких ключових ділянках, повинні мати достатній досвід роботи;

- повсякденний візуальний контроль адміністраторів безпека за станом опечатування системних блоків, що зводить до мінімуму ризик несанкціонованого підключення до ЗОТ;

- обмеження складу встановленого програмного забезпечення та апаратних засобів відповідними затвердженими переліками, ведення паспортів на всі автоматизовані системи, де відбиваються всі відомості щодо складу їх програмного та апаратного забезпечення, а також наявність регулярних звірок паспортних даних з реальними.

Модель порушника для АС класу «1» наведена у Таблицях 4.2.1 – 4.2.6.

В наведених таблицях рівень загроз характеризується наступними категоріями: 1 - незначні; 2 - значимі, але припустимі; 3 - середні; 4 - дуже значні.

Таблиця 4.2.1.

Класифікація порушника за мотивом порушення

Позначення	*Мотив порушення*	*Рівень загрози*
М1	*Безвідповідальність*	*1*

М2	*Самозатвердження*	*2*
М3	*Корисливий інтерес*	*3*
М4	*Професійний обов'язок*	*4*

Таблиця 4.2.2.

Класифікація порушника за кваліфікацією

Позначення	*Основні кваліфікаційні ознаки порушника*	*Рівень загрози*
К1	*Знає функціональні особливості системи, основні закономірності формування інформаційних ресурсів та потоків запитів до них, має навички щодо користування штатними засобами системи*	*1*
К2	*Володіє високим рівнем знань та практичними навичками роботи з технічними засобами системи та їх обслуговування.*	
К3	*Володіє високим*	

	рівнем знань в галузі програмування та обчислювальної техніки, проектування та експлуатації автоматизованих інформаційних систем	
К4	*Знає структуру, функції та механізми дії засобів захисту і їх недоліки*	
К5	*Знає недоліки та «вади» механізмів захисту, які вбудовані у системне програмне забезпечення та його не документовані можливості*	
К6	*Є розробником програмних та апаратно-програмних засобів захисту або системною програмного*	

	забезпечення	

Таблиця 4.2.3.

Класифікація порушника за методами та засобами порушення безпеки інформації

Позначення	*Основні кваліфікаційні ознаки порушника*	*Рівень загрози*
31	*Використовує лише агентурні методи одержання відомостей*	
32	*Використовує пасивні засоби (технічні засоби перехоплення інформації без модифікації компонентів системи)*	
33	*Використовуй лише штатні засоби та недоліки системи захисту для подолання (несанкціоновані дії з використанням дозволених засобів), а також компактні носії*	

	інформації, які можуть бути приховані пронесені крізь охорону	
34	*Застосовує методи та засоби дистанційного (з використанням штатних каналів та протоколів зв'язку) упровадження програмних закладок та спеціальних резидентних програм збору, пересилання або блокування даних, дезорганізації системи обробки інформації*	
35	*Застосовує методи та засоби активного впливу (модифікація та підключення додаткових технічних засобів, підключення до каналів передачі*	

	даних)	

Таблиця 4.2.4.

Кваліфікація порушника за часом дії

Позначення	*Основні кваліфікаційні ознаки порушника*	*Рівень загрози*
Ч1	*До впровадження АС або її окремих компонентів*	*1*
Ч2	*Під час бездіяльності компонентів системи (у неробочій час планових перерв у роботі, перерв для обслуговування та ремонту тощо)*	
Ч3	*Під час функціонування АС (або компонентів системи)*	
Ч4	*Як у процесі функціонування АС, так і під час призупинки роботи системи*	

Таблиця 4.2.5.

Кваліфікація порушника за місцем дії

Позначення	*Основні кваліфікаційні ознаки порушника*	*Рівень загрози*
Д1	*Без допуску на контрольовану територію організації*	*1*
Д2	*З контрольованої території без допуску в будинки та споруди*	
Д3	*Усередині приміщень, але без допуску до технічних засобів АС*	
Д4	*З робочих місць користувачів АС*	
Д5	*З доступом у зони даних*	
Д6	*З доступом у зону керування засобами забезпечення*	

	безпеки АС	

Таблиця 4.2.6.

Профілі можливостей порушників безпеки інформації

Визначення категорій порушника	*Потенціальний рівень загрози*	*Характер дій порушника*					*Ефективний рівень загроз*
		Мотив порушення	*Кваліфікації*	*Можливості*	*Час дії*	*Місце дії*	
Технічний персонал, який обслуговує будови та приміщення (електрики, сантехніки, прибиральники тощо), в яких розташовані компоненти АС		*М1*	*-*	*З1*	*Ч2*	*Д3*	
Персонал, який обслуговує технічні засоби (інженери, техніки)		*М1*	*К2*	*З3*	*Ч4*	*Д6*	
Користувачі АС.		*М1*	*К1*	*З3*	*Ч3*	*Д4*	
Співробітники підрозділів розробки та супроводження програмного забезпечення		*М2*	*К3*	*З3*	*Ч1*	*Д6*	
Співробітники служби захисту інформації.		*М1*	*К5*	*З3*	*Ч4*	*Д6*	

9.6. Звіт про виконання лабораторної роботи подати у вигляді документу, в який входить один підрозділ:

4.2. Модель порушника.

Лабораторна робота № 10
Підготовка розділу 5 «Плану захисту інформації в автоматизованій системі».

Завдання лабораторної роботи:

10.1. Ознайомитися з вимогами розділу 5 додатку **«**План захисту інформації в автоматизованій системі**».** до НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі».

10.2. Застосовуючи положення та вимоги, викладені у розділі 5 зазначеного додатку, розробити: Розділ 5. «Політика безпеки інформації в АС», який повинен входити до «Плану захисту інформації в автоматизованій системі» зазначеній у вступі лабораторного практикуму.

10.3. Розділ 5. «Політика безпеки інформації в АС» виконується за нижченаведеним зразком.

Зразок

Розділ5. Політика безпеки інформації в АС

5.1. Організаційні заходи

Організаційні заходи захисту інформації – це комплекс адміністративних і обмежувальних заходів, спрямованих на оперативне вирішення завдань захисту інформації шляхом регламентації діяльності персоналу і порядку функціонування

засобів забезпечення інформаційної діяльності, а також засобів забезпечення захисту інформації. До складу організаційних входять такі заходи:

5.1.1. Забезпечення основних вимог до обладнання приміщень, в яких розташовані АС. Приміщення, в яких розміщуються АС (назва підприємства), мають:

- капітальні стіни і надійне перекриття між поверхами;

- міцні двері з двома замками;

- подвійні рами з внутрішніми замками, а також штори або жалюзі на вікнах;

- сигналізацію, виведену на пост охорони;

- визначений порядок фізичного доступу до технічних засобів АС.

5.1.2. Призначення ролей співробітників, що мають відповідні повноваження і виконують функції:

- користувачів АС;

- складу служби захисту інформації (керівника служби захисту інформації _____ та позаштатних адміністраторів безпеки).

5.1.3. Розроблення службою захисту інформації і затвердження інструкцій, що визначають:

- *порядок відвідування АС особами, що безпосередньо не беруть участь в процесі обробки інформації (у тому числі для проведення ремонтно- профілактичних робіт);*
- *порядок відкриття приміщень у неробочий час та у разі введення воєнного чи надзвичайного стану;*
- *порядок евакуації та знищення МНД, АС та документації до них у разі введення воєнного чи надзвичайного стану;*
- *забезпечення режиму обробки інформації в АС _____;*

5.1.4. Розроблення службою захисту інформації і затвердження правил генерації паролів.

Паролі можуть генеруватися адміністратором безпеки АС, відповідно до встановленої керівництвом періодичності. Вимоги до структури, порядок присвоєння і використання паролів визначаються керівництвом та відображаються в Інструкціях адміністратору безпеки та користувачам АС.

5.1.5. Забезпечення вимог до обладнання АС:

- АС, що призначені для обробки ІзОД, являються не зв'язаними між собою відокремленими ПЕОМ, тобто відносяться до АС класу «1». Кожна ПЕОМ має склад обладнання та конфігурацію відповідно до формулярів АС;

- кожна ПЕОМ підключається до системи заземлення, яка відповідає вимогам НД ТЗІ через роз'єм живлення;

5.1.6 Організація навчання персоналу і підвищення його кваліфікації.

Для АС _____ на випадок виникнення надзвичайних ситуацій розроблена та затверджена Інструкція, яка передбачає:

- *порядок оповіщення посадових осіб;*
- *дії персоналу в кожній конкретній нештатній ситуації;*
- *порядок відкриття приміщень, в яких розміщені технічні засоби і резервні копії інформаційних фондів АС;*
- *порядок допуску на територію робочих ділянок АС працівників пожежної і інших аварійних служб;*

5.2. Реалізація елементів КСЗІ системними програмними засобами

В АС _____, призначеної для обробки ІзОД, використовується програмний засіб захисту «Лоза-1», («Гриф-1»).

5.3. Система управління доступом до ресурсів

5.3.1. Нормативні і організаційні основи функціонування системи управління доступом до ресурсів АС.

Управління доступом є одним з основних заходів запобігання несанкціонованому доступу до ресурсів (функціональних програмних комплексів, технічних засобів та інформаційних об'єктів) АС.

Функції управління доступом в АС можуть реалізуватися відповідним комплексом спеціальних програмних засобів – системою управління доступом (СУД), яка входить до складу програмного забезпечення АС («Лоза-1», «Гриф-1»).

5.3.2. Суб'єкти системи управління доступом до ресурсів.

Управління доступом до інформаційних об'єктів (ІО) в АС реалізується за принципом прямого доступу користувачів до ресурсів АС відповідно до заздалегідь обумовлених повноважень.

Користувачами АС є співробітники, уповноважені директором _____ (призначаються наказом) здійснювати ті або інші операції з обробки інформації. Характер зазначених операцій задається доступними програмними засобами і встановлюється відповідно до посадових обов'язків і повноважень цього користувача.

З числа користувачів виділяються особи, наділені особливими повноваженнями із доступу до ресурсів АС – адміністратори безпеки АС (позаштатні адміністратори безпеки АС). Адміністратор здійснює загальне керівництво роботою АС та контролює відповідність порядку

функціонування АС вимогам нормативних документів. Адміністратор також відповідає за її працездатність, визначає регламент технічного обслуговування програмних і технічних засобів АС, здійснює оперативний контроль за роботою користувачів і функціонуванням СУД, здійснює поточну і регулярну перевірку повноважень користувачів і їх коригування відповідно до змін у штатному розкладі з повідомленням про це користувачів.

5.3.3. Функції управління і контролю.

Контроль функціонування СУД в АС здійснює адміністратор безпеки підрозділу, за якими закріплена дана АС. Загальний контроль функціонування СУД АС _____ здійснює керівник служби захисту інформації.

Адміністратор безпеки здійснює контроль за відповідністю даних системного журналу встановленим нормативам, фіксує всі спроби НСД, вживає заходи для запобігання або ліквідації їхніх наслідків, встановленим порядком інформує про ці спроби керівника служби захисту інформації і свого безпосереднього керівника та проводить за їх вказівкою відповідне розслідування (спільно з керівником служби захисту інформації).

Реалізація функцій СУД дозволяє адміністратору здійснювати:

- *створення і видалення користувачів;*
- *встановлення атрибутів доступу користувачів до ресурсів АС;*
- *конфігурацію програмних і апаратних засобів АС.*

5.4. Система забезпечення цілісності інформації

5.4.1. Заходи захисту від закладних програм і комп'ютерних вірусів.

На етапі введення АС в експлуатацію здійснюється атестація програмних засобів на відповідність вимогам ТЗ.

На цьому ж етапі керівником служби захисту інформації в АС визначаються:

- *перелік програмних засобів, дозволених до інсталяції (у тому числі антивірусних);*
- *порядок використання програмних засобів;*
- *дії персоналу у випадку виявлення відхилень у функціонуванні інстальованого програмного забезпечення.*

По кожному факту виявлення на робочих місцях комп'ютерних вірусів у встановленому порядку проводять службове розслідування.

5.4.2. Забезпечення безперебійного функціонування технічних і програмних засобів АС.

Метою забезпечення безперебійного й безвідмовного функціонування технічних і програмних засобів АС є зведення до мінімуму випадків відмови в обслуговуванні.

Безперебійність функціонування технічних і програмних засобів АС _____ досягається:

- *своєчасним проведенням регламентних робіт на технічних засобах кожної АС (відповідно до експлуатаційної документації);*
- *створенням резервних копій програмних засобів;*
- *тестуванням апаратних і програмних засобів АС на виконання ними своїх функцій.*

Тестування проводиться адміністратором безпеки періодично (один раз у квартал) після проведення регламентних і ремонтних робіт на технічних засобах АС та позапланово –

після виникнення будь-яких ситуацій, у результаті яких порушилася або могла бути порушена їх працездатність.

5.4.3. Резервування інформації.

Створення резервних копій інформаційних фондів здійснюється способом, що мінімізує матеріальні витрати і втрати при відновленні інформації, для чого передбачається зняття з заданою періодичністю двох повних їх копій.

Копії інформаційних фондів зберігаються в різних приміщеннях, по можливості максимально віддалених одне від одного. Розробляється інструкція, що визначає порядок резервування інформації і порядок її відновлення з використанням резервних копій у разі потреби.

10.4. Звіт про виконання лабораторної роботи подати у вигляді документу, в який входить один розділ:

5. Політика безпеки інформації в АС.

Лабораторна робота № 11
Підготовка «Акту категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці»

Завдання лабораторної роботи:

11.1. Ознайомитися з вимогами НД ТЗІ 1.6-005-2013 «Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці».

11.2. Застосовуючи положення та вимоги, викладені в НД ТЗІ 1.6-005-2013, розробити: «Акт категоріювання АС», зазначеної у вступі лабораторного практикуму.

11.3. Під час виконання лабораторної роботи як форми акта використовувати Додаток А до НД ТЗІ 1.6-005-2013

«Захист інформації на об’єктах інформаційної діяльності. Положення про категоріювання об’єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці».

11.4. Звіт про виконання лабораторної роботи подати як документ, що містить «Акт категоріювання АС ____ (назва організації)». Підготовлений Акт у інших номінальних учасників процесу категоріювання не підписувати.

Лабораторна робота № 12
Підготовка «Акту обстеження на об’єкті інформаційної діяльності»

Завдання лабораторної роботи:

12.1. Ознайомитися з вимогами НД ТЗІ 3.1-001-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні роботи

12.2. Застосовуючи положення та вимоги, викладені в НД ТЗІ 3.1-001-07, розробити: «Акт обстеження на об’єкті інформаційної діяльності», для АС зазначеної у вступі лабораторного практикуму.

12.3. Форма та зміст Акту обстеження на об’єкті інформаційної діяльності стосовно створення комплексу ТЗІ приведено в Додатку А до НД ТЗІ НД ТЗІ 3.1-001-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні роботи.

12.4. Лабораторну роботу доцільно виконати, користуючись нижченаведеним зразком.

Зразок

Директор

_____ (назва організації)
"___" _____ 20__ р.

АКТ
за результатами обстеження об'єкта ЕОТ – автоматизованої системи класу «1», яка знаходиться в приміщенні № _____ (назва організації)

1. Об'єкту надано четверту категорію (Акт категоріювання автоматизованої системи класу «1» _____ (назва організації) № 9 від р., Акт категоріювання приміщення, де розміщена автоматизована система класу «1» _____ (назва організації, № ___ від ___ р.).

2. Характеристика об'єкту інформаційної діяльності.

Об'єкт інформаційної діяльності (далі – ОІД) знаходиться в м._____ та складається з автоматизованої системи класу «1», яка розміщена у виділеному приміщенні № _____ (назва організації) Виділене приміщення розташоване на __поверсі __-ти поверхової будівлі _____ (назва організації). Кабінет № виходить вікнами у бік вулиці_____.

Контрольована зона визначена наказом директора _____ (назва організації) від___ р. №___.

Межа контрольованої зони (КЗ) у всіх напрямках обмежується територією _____ (назва організації)

Охорона та пропускний режим людей та автотранспортних засобів на територію _____ (назва організації) здійснюється відповідальним черговим відділу оперативно-чергової служби зв'язку та оповіщення управління оперативно-чергової служби _____ (назва організації). Він діє цілодобово і здійснює контроль за проїздом, проходом і переміщенням рухомих засобів та осіб в межах території підприємства.

В таблиці 1 наведено дані щодо характеристик вулиць, що проходять поруч з будинком, в якому знаходиться ОІД.

Фундамент будинку – залізобетонний, стіни – цегляні. Перекриття між поверхами виконані із залізобетонних плит розміром 630х120х30 см.

Електроживлення здійснюється від трансформаторної підстанції ТП-10, що розміщена поза межами контрольованої зони на вулиці. Теплопостачання здійснюється від системи теплопостачання, яка розташована поза територією контрольованої зони. Водопостачання та каналізація підключені до міських мереж. Територія навколо будинку впорядкована, має асфальтне покриття та зелену зону. Контури заземлення виконані усередині КЗ.

На відстані, що дорівнює або менша ніж 200 метрів від _____ (назва організації) відсутні іноземні представництва, які користуються правом недоторканості (лист Управління Держспецзв'язку в Рівненській обл.).

Вікно в приміщенні – 1 вікно, яке виходить до вул. ___ . Вхідні двері до кабінету – металеві та другі двері з середини кабінету – дерев'яні. Батарея опалення – одна батарея, що розташована під вікном.

Кабінет обладнаний системами електроживлення, заземлення, освітлення, пожежною та охоронною сигналізаціями, системами теплопостачання та водопостачання.

Системи електроживлення, теплопостачання та водопостачання мають вихід за межі контрольованої зони.

На стелі закріплено датчики пожежної сигналізації. В наявності датчик руху та датчик на розкриття двері. Пожежна сигналізація не має виходу за межі контрольованої зони та виведена на пульт сигналізації чергового.

3. Опис суміжних з приміщенням №__ приміщень.

Приміщення №__ має такі суміжні приміщення:

- *праворуч – приміщення № ();*
- *зліва – приміщення № (заступник директора);*
- *зверху – приміщення № (начальник)*
- *знизу – приміщення № 7 (заступник начальника)*

Ні в суміжному приміщенні, ні в корпусі в цілому не працюють іноземні громадяни, неконтрольоване перебування сторонніх осіб унеможливлено.

4. *Склад технічних засобів АС класу «1» 4 категорії (ПЕОМ, периферійних пристроїв) наведено в таблиці 1.*

Таблиця 1

Склад технічних засобів

Пристрій	***Тип***	***Номер***

На АС встановлено операційну систему сімейства Windows (Windows 7,… 10) та антивірусний програмний засіб ____(… версія), який має експертний висновок Держспецзв'язку України від ___№ __ (код реєстрації продукту____, марка: _).).

Крім цього, на зазначеній АС встановлено функціональне програмне забезпечення, призначене для опрацювання текстових документів, електронних таблиць та інше

Як захист від несанкціонованого доступу до ресурсів АС використовується комплекс засобів захисту від несанкціонованого доступу «Лоза-1» («Гриф-1») версії __, конфігурації __що має Експертний висновок Держспецзв'язку України № від року.

5. Електроживлення об'єкту здійснюється від трансформаторної підстанції ТП-10, яка знаходиться поза межами контрольованої зони.

7. АС заземлена – контур заземлення розташовано в межах контрольованої зони.

Висновок:

За результатами обстеження підтверджується можливість розгортання на об'єкті створюваної АС.

Голова комісії: _____;
Члени комісії: _____;
_____;

12.5. Звіт про виконання лабораторної роботи подати як документ, що містить «Акт обстеження на об'єкті інформаційної діяльності щодо створення комплексу ТЗІ ____ (назва організації)». Підготовлений Акт в інших номінальних учасників процесу обстеження не підписувати.

Лабораторна робота № 13
Здійснення класифікації автоматизованої системи та вибір функціональних профілів захищеності

Завдання лабораторної роботи:

13.1. Ознайомитися з вимогами НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності інформації від

несанкціонованого доступу та НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.

13.2. Застосовуючи положення та вимоги, викладені в розділі 5 «Класифікація автоматизованих систем» НД ТЗІ 2.5-005-99, класифікувати АС, зазначену у вступі лабораторного практикуму, дати її визначення та істотні особливості.

13.3. Застосовуючи положення та вимоги, викладені в підрозділі 7.1.5 «Стандарті функціональні профілі захищеності в КС, що входять до складу АС класу 1, головною вимогою до яких є забезпечення конфіденційності і доступності оброблюваної інформації» НД ТЗІ 2.5-005-99 студентам, які мають непарні номери в списку групи вибрати 3-й рівень профілю; студентам, які мають парні номери в списку групи вибрати 4-й рівень профілю.

13.4. Користуючись положеннями та вимогами, викладеними в розділах 5 – 9 НД ТЗІ 2.5-004-99. «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу», знайти та привести у відповідність вибраним у п. 13.3 рівням послуг їх назви.

13.5. Лабораторну роботу доцільно виконати, користуючись нижченаведеним зразком.

Зразок

1. Автоматизована система _____(назва організації) належить до Класу «1» — Одномашинний однокористувачевий комплекс, який обробляє інформацію однієї або кількох ступенів обмеження доступу.

Істотні особливості:

- *в кожний момент часу з комплексом може працювати тільки один користувач, хоч у загальному*

випадку осіб, що мають доступ до комплексу, може бути декілька;

- *користувачі можуть мати різні повноваження (права) щодо доступу до інформації, яка обробляється.*

2. Стандартні функціональні профілі захищеності в КС, що входять до складу АС _____(назва організації) класу 1, з підвищеними вимогами до забезпечення конфіденційності, цілісності і доступності інформації:

1.КЦД.1 = {КА-1, КО-1, ЦА-1, ЦО-1, ДР-1, ДВ-1, НР-2, НИ-2, НК-1, НО-1, НЦ-1, НТ-1}

КА-1 – Базова адміністративна конфіденційність;
КО-1 – Повторне використання об'єктів;
ЦА-1 – Мінімальна адміністративна цілісність;
ЦО-1 – Обмежений відкат;
ДР-1 – Квоти;
ДВ-1 – Ручне відновлення;
НР-2 – Захищений журнал;
НИ-2 – Множинна ідентифікація і автентифікація;
НК-1 – Однонаправлений достовірний канал;
НО-1 – Розподіл обов'язків адміністраторів;
НЦ-1 – КЗЗ з контролем цілісності;
НТ-1 – Самотестування за запитом.

13.6. Звіт про виконання лабораторної роботи подати як документ, що містить 2 пункти: 1 – класифікація АС, 2 – Стандартні функціональні профілі захищеності КС.

Лабораторна робота № 14
Опис функціональних профілів захищеності

Завдання лабораторної роботи:

14.1. Ознайомитися з вимогами НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.

14.2. Застосовуючи положення та вимоги, викладені в розділах 5 – 9 НД ТЗІ 2.5-004-99. «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу», надати описи наступних функціональних профілів захищеності з деталізацією кожної функціональної послуги:

- КА-1

- КО-1

14.3. Лабораторну роботу доцільно виконати, використуючи нижченаведений зразок.

Зразок

Профілі захищеності інформації КА-2, КО-0

Базова адміністративна конфіденційність (КА-2)

Політика реалізації послуги повинна розповсюджуватися на користувачів всіх ролей і такі об'єкти захисту:

- дані у вигляді файлів різних форматів, які містять відомості, що становлять державну таємницю;

- дані з обмеженим доступом у вигляді файлів різних форматів, які не містять відомостей, що становлять державну таємницю (службова інформація, конфіденційна інформація тощо);

- технологічна інформація, яка використовується для забезпечення функціонування АС та КЗЗ (файли налаштування програмного забезпечення ПЕОМ, списки зареєстрованих користувачів, їх ідентифікатори, журнали реєстрації подій тощо);

- функціональні задачі (процеси), умежах яких користувач працює з об'єктами файлової системи.

Розмежування доступу користувачів до об'єктів захисту повинно здійснюватися на підставі атрибутів доступу користувача та об'єкта захисту.

Запити на зміну прав доступу повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністратора безпеки.

КЗЗ повинен надавати можливість адміністратору безпеки для кожного об'єкта захисту визначити конкретних користувачів і/або групи користувачів, які мають право одержувати інформацію від об'єкта захисту.

КЗЗ повинен надавати можливість адміністратору безпеки для кожного процесу, який використовується для обробки об'єктів захисту, визначити конкретних користувачів і/або групи користувачів, які мають право ініціювати процес.

Права доступу для кожного об'єкта захисту повинні встановлюватися в момент його створення.

Повторне використання захищених об'єктів (КО-0)

До множини захищених об'єктів повинні відноситися сегменти оперативної пам'яті та пам'яті на магнітних, оптичних та флеш носіях інформації, які використовуються системними та прикладними програмами, що здійснюють оброблення секретної інформації.

Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт:

- встановлені для попереднього користувача або процесу права доступу до цього об'єкта повинні бути скасовані;

семантичний зміст інформації, що міститься в цьому об'єкті, повинен стати недосяжним.

14.4. Звіт про виконання лабораторної роботи подати у вигляді документу Опис функціональних профілів захищеності інформації КА-1, КО-1.

Лабораторна робота № 15
Опис функціональних профілів захищеності

Завдання лабораторної роботи:

15.1. Ознайомитися з вимогами НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.

15.2. Застосовуючи положення та вимоги, викладені в розділах 5 – 9 НД ТЗІ 2.5-004-99. «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу», надати описи наступних функціональних профілів захищеності з деталізацією кожної функціональної послуги:

- ДР-2;

- ДС-2, або ДС-3 (залежно від варіанта).

15.3. Лабораторну роботу доцільно виконати, використуючи нижченаведений зразок.

Зразок

Профілі захищеності інформації ДР-2, ДС-2(3)

Мінімальна адміністративна цілісність (ЦА-1)

Політика реалізації послуги повинна розповсюджуватися на користувачів всіх ролей і такі об'єкти захисту:

- дані у вигляді файлів різних форматів, які містять відомості, що становлять державну таємницю;

- дані з обмеженим доступом у вигляді файлів різних форматів, які не містять відомостей, що становлять державну таємницю (службова інформація, конфіденційна інформація тощо);

- технологічна інформація, яка використовується для забезпечення функціонування АС та КЗЗ (файли налаштування програмного забезпечення ПЕОМ, списки зареєстрованих користувачів, їх ідентифікатори, журнали реєстрації подій тощо);

- відкрита інформація.

Розмежування доступу користувачів до об'єктів захисту повинно здійснюватися на підставі атрибутів доступу користувача та об'єкта захисту.

Запити на зміну прав доступу повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністратора безпеки.

КЗЗ повинен надавати можливість адміністратору безпеки для кожного об'єкта захисту визначити конкретних користувачів і/або групи користувачів, які мають право модифікувати об'єкт захисту.

Права доступу для кожного об'єкта захисту повинні встановлюватися в момент його створення.

15.4. Звіт про виконання лабораторної роботи подати у вигляді документу Опис функціональних профілів захищеності інформації ДР-2, ДС-2(3), залежно від варіанта.

Лабораторна робота № 16
Опис функціональних профілів захищеності

Завдання лабораторної роботи:

16.1. Ознайомитися з вимогами НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.

16.2. Застосовуючи положення та вимоги, викладені в розділах 5–9 НД ТЗІ 2.5-004-99. «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу», надати описи наступних функціональних профілів захищеності з деталізацією кожної функціональної послуги:

- ДЗ-2 або ДЗ-3 (залежно від варіанта);

- ДВ-2, або ДВ-3 (залежно від варіанта).

16.3. Лабораторну роботу доцільно виконати, використовуючи нижченаведений зразок.

Зразок

Профілі захищеності інформації ДЗ-2(3), ДВ-2(3)
Ручне відновлення (ДВ-1)

До переліку подій, після здійснення яких КЗЗ має переводити АС у стан блокування подальшої роботи, повинні бути внесені відмови або переривання процесів завантаження АС, ініціації та перевірки цілісності КЗЗ, процедур автентифікації користувачів, процедур ведення журналу реєстрації подій.

Повернення АС до нормального функціонування може бути здійснено тільки після втручання адміністратора безпека.

Повторна інсталяція КЗЗ можлива після копіювання адміністратором безпеки журналу подій на носій інформації для проведення аналізу можливих фактів порушень політики безпеки. Інсталяція КЗЗ здійснюється системним адміністратором за участю адміністратора безпеки. За результатами робіт складається відповідний акт.

В інструкціях адміністраторів (у частині, що їх стосується) та в Плані захисту інформації повинен бути

визначений порядок створення резервних копій інформації, періодичність створення таких копій, порядок поводження з носіями резервних копій інформації, порядок відновлення інформації після збоїв компонентів АС.

Модернізація (ДЗ-1)

Ця послуга дозволяє гарантувати доступність АС у цілому, окремих процесів й об'єктів, можливість використання інформації в процесі заміни окремих компонентів.

Політика модернізації, що реалізується КЗЗ, поширюється на системне та функціональне програмне забезпечення, технологічну інформацію, яка використовується для забезпечення функціонування АС та КЗЗ. Послуга гарантує, що модернізація АС не призведе до компрометації політики безпеки інформації в АС.

Політика проведення модернізації АС повинна надавати можливість проведення модернізації АС адміністратору безпеки або іншому адміністратору, а також визначення для кожного з них повноваження та множину виконуваних ними допустимих операцій з метою модернізації АС.

Модернізація окремих компонентів АС не повинна призводити до необхідності проведення повторної інсталяції програмного забезпечення цих компонентів або до переривання виконання КЗЗ функцій захисту.

16.4. Звіт про виконання лабораторної роботи подати як документ Опис функціональних профілів захищеності інформації ДЗ-2 (3), ДВ-2 (3), залежно від варіанта.

Лабораторна робота № 17
Опис функціональних профілів захищеності

Завдання лабораторної роботи:

17.1. Ознайомитися з вимогами НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.

17.2. Застосовуючи положення та вимоги, викладені в розділах 5 – 9 НД ТЗІ 2.5-004-99. «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу», надати описи наступних функціональних профілів захищеності з деталізацією кожної функціональної послуги: **НР-3 або НР-4** (залежно від варіанта); **НИ-2, НК-1**

17.3. Лабораторну роботу доцільно виконати, використовуючи нижченаведений зразок.

Зразок

Профілі захищеності інформації НР-2, НК-1, НИ-3

Захищений журнал (НР-2)

КЗЗ повинен бути здатним здійснювати реєстрацію таких подій, що мають безпосереднє відношення до безпеки:

- реєстрацію та видалення із системи користувачів (псевдонім користувача, дата, час);

- результати автентифікації користувачів: вхід/вихід користувача в систему/із системи, невдалі спроби автентифікації (псевдонім користувача, дата, час);

- зміну пароля (псевдонім користувача, дата, час);

- надання та зміну прав доступу до інформаційного об'єкта та його обробки (псевдонім користувача, значення атрибутів доступу інформаційного об'єкта, дата, час);

- виведення документа на принтер (псевдонім користувача, ідентифікатор інформаційного об'єкта, дата, час);

- експорт об'єктів захисту на з'ємні магнітні, оптичні та флеш носії інформації (псевдонім користувача,

ідентифікатор інформаційного об'єкта, серійний номер носія інформації, дата, час);

- спроби несанкціонованих дій з інформацією (псевдонім користувача, дата, час, назва інформаційного об'єкта, до якого були спроби отримати несанкціонований доступ або виконати несанкціоновані дії);

- виявлення фактів порушення цілісності КЗЗ (код порушення, псевдонім користувача, дата, час).

КЗЗ повинен забезпечувати захист журналу реєстрації від несанкціонованого ознайомлення, модифікації або знищення.

Адміністратори повинні мати в своєму розпорядженні засоби перегляду і аналізу журналів реєстрації.

Однонаправлений достовірний канал (НК-1)

Достовірний канал повинен використовуватися для початкової ідентифікації та автентифікації користувачів. Зв'язок із використанням цього каналу має бути ініційований виключно користувачем.

Множинна ідентифікація та автентифікація (НИ-3)

Кожний користувач повинен однозначно ідентифікуватися КЗЗ на підставі введеного імені (псевдоніму).

Перш ніж дозволити будь-якому користувачу виконувати будь-які інші, контрольовані КЗЗ дії, КЗЗ повинен автентифікувати цього користувача на підставі введеного ним пароля та наданого фізичного ідентифікатора.

Для визначення псевдоніму та пароля повинна використовуватися буквенно-цифрова клавіатура. Кількість символів у паролі повинна бути не менше 8.

КЗЗ має забезпечувати захист даних автентифікації від несанкціонованого ознайомлення, модифікації або руйнування.

17.4. Звіт про виконання лабораторної роботи подати як документ Опис функціональних профілів захищеності інформації НР-3 (4), залежно від варіанта, НИ-2, НК-1.

Лабораторна робота № 18
Опис функціональних профілів захищеності

Завдання лабораторної роботи:

18.1. Ознайомитися з вимогами НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.

18.2. Застосовуючи положення та вимоги, викладені в розділах 5 – 9 НД ТЗІ 2.5-004-99. «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу», надати описи наступних функціональних профілів захищеності з деталізацією кожної функціональної послуги: **НЦ-1, НО-2, НТ-2.**

18.3. Лабораторну роботу доцільно виконати, використовуючи нижченаведений зразок.

Зразок

Профілі захищеності інформації НЦ-1, НО-2, НТ-2

КЗЗ із контролем цілісності (НЦ-1)

Політика контролю цілісності, яка реалізується КЗЗ, повинна належати до компонентів програмного забезпечення АС, які задіяні для реалізації механізмів КЗЗ.

Контроль цілісності програм та даних, що входять до складу КЗЗ, повинен здійснюватися при кожному включенні АС або завантаженні операційної системи. Контроль полягає у перевірці наявності всіх зазначених компонентів та відповідності їх характеристик еталонним значенням.

У разі виявлення порушення цілісності будь-якого із своїх компонентів КЗЗ повинен зареєструвати цю подію у журналі реєстрації і (або) автоматично відновити відповідність

компонента еталону або привести АС до стану, з якого повернути АС до нормального функціонування може лише адміністратор безпеки.

З метою недопущення порушення політики безпеки необхідно унеможливити використання в АС програмного забезпечення, яке не має відповідного дозволу та не призначене для обробки секретної інформації, зокрема засобів налагодження програмного забезпечення, засобів моніторингу за процесами та ресурсами АС тощо.

Розподіл обов'язків адміністраторів (НО-2)

Повинні бути визначені ролі адміністратора та звичайного користувача і притаманні їм функції.

Політика розподілу обов'язків повинна визначати мінімум дві адміністративні ролі: адміністратора безпеки та системного адміністратора. Функції, притаманні кожній із ролей, повинні бути мінімізовані так, щоб містити лише ті функції, які необхідні для виконання цієї ролі.

Роль звичайного користувача повинна бути обмежена функціями, необхідними для роботи із захищеними даними.

Фізична особа повинна мати можливість виступати в певній ролі тільки в тому разі, якщо у процесі автентифікації вона визначена як особа, якій притаманна ця роль.

Самотестування під час старту (НТ-2)

Політика самотестування, яка реалізується КЗЗ, повинна належати до компонентів програмного забезпечення АС, які задіяні для реалізації механізмів КЗЗ.

Повинні бути реалізовані процедури, які призначені для оцінки правильності функціонування КЗЗ.

КЗЗ має бути здатним виконувати набір тестів для оцінки правильності функціонування своїх критичних функцій. Тести повинні виконуватися за запитом адміністратора безпеки та при ініціації КЗЗ.

ЛІТЕРАТУРА

1. Грайворонський М. В., Новіков О. М Безпека інформаційно-комунікаційних систем. Київ : БХВ. 2009, 596 с.

2. Нормативі документи з технічного захисту інформації. URL: http://www.dsszzi.gov.ua/dsszzi-/control/uk/publish/article?art_id=89740&cat_id=89734.